

Rec'd PCT/PTO

03 SEP 2004

PCT/JP03/02525

#2

日 本 国 特 許 庁

04.03.03

JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 3月 5日

REC'D 25 APR 2003

WIPO

PCT

出 願 番 号

Application Number:

特願2002-059179

[ST.10/C]:

[JP2002-059179]

出 願 人

Applicant(s):

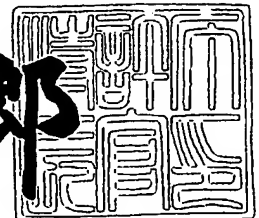
三洋電機株式会社
シャープ株式会社
日本ビクター株式会社
パイオニア株式会社
株式会社日立製作所
フェニックステクノロジーズ株式会社
富士通株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2003年 4月 8日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田信一郎



BEST AVAILABLE COPY

出証番号 出証特2003-3024279

【書類名】	特許願
【整理番号】	1020002
【提出日】	平成14年 3月 5日
【あて先】	特許庁長官殿
【国際特許分類】	H04M 11/08
【発明者】	
【住所又は居所】	大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内
【氏名】	堀 吉宏
【発明者】	
【住所又は居所】	大阪府大阪市阿倍野区长池町2番22号 シャープ株式会社内
【氏名】	大野 良治
【発明者】	
【住所又は居所】	神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内
【氏名】	大石 剛士
【発明者】	
【住所又は居所】	埼玉県所沢市花園4丁目2610番地 パイオニア株式会社 所沢工場内
【氏名】	戸崎 明宏
【発明者】	
【住所又は居所】	埼玉県所沢市花園4丁目2610番地 パイオニア株式会社 所沢工場内
【氏名】	多田 謙一郎
【発明者】	
【住所又は居所】	神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所 システム開発研究所内
【氏名】	平井 達哉

【発明者】

【住所又は居所】 東京都新宿区新宿 4 - 2 - 1 8 新宿光風ビル 6 F フ
ェニックステクノロジー株式会社内

【氏名】 津留 雅文

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通
株式会社内

【氏名】 長谷部 高行

【特許出願人】

【識別番号】 000001889

【住所又は居所】 大阪府守口市京阪本通 2 丁目 5 番 5 号

【氏名又は名称】 三洋電機株式会社

【特許出願人】

【識別番号】 000005049

【住所又は居所】 大阪府大阪市阿倍野区长池町 2 2 番 2 2 号

【氏名又は名称】 シャープ株式会社

【特許出願人】

【識別番号】 000004329

【住所又は居所】 神奈川県横浜市神奈川区守屋町 3 丁目 1 2 番地

【氏名又は名称】 日本ビクター株式会社

【特許出願人】

【識別番号】 000005016

【住所又は居所】 東京都目黒区目黒 1 丁目 4 番 1 号

【氏名又は名称】 パイオニア株式会社

【特許出願人】

【識別番号】 000005108

【住所又は居所】 東京都千代田区神田駿河台 4 丁目 6 番地

【氏名又は名称】 株式会社日立製作所

【特許出願人】

【識別番号】 300017636
【住所又は居所】 東京都新宿区新宿 4 - 2 - 1 8 新宿光風ビル 6 F
【氏名又は名称】 フェニックステクノロジーズ株式会社

【特許出願人】

【識別番号】 000005223
【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号
【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100064746
【弁理士】
【氏名又は名称】 深見 久郎

【選任した代理人】

【識別番号】 100085132
【弁理士】
【氏名又は名称】 森田 俊雄

【選任した代理人】

【識別番号】 100091409
【弁理士】
【氏名又は名称】 伊藤 英彦

【選任した代理人】

【識別番号】 100096781
【弁理士】
【氏名又は名称】 堀井 豊

【手数料の表示】

【予納台帳番号】 008693
【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】

図面 1

【物件名】

要約書 1

【プルーフの要否】

要

【書類名】 明細書

【発明の名称】 データ記憶装置

【特許請求の範囲】

【請求項 1】 機密データを保護するための所定の入出力手順に従って前記機密データの入出力を行ない、かつ、前記機密データを記憶するデータ記憶装置であって、

外部とデータのやり取りを行なうインターフェース手段と、

前記機密データを記憶する第 1 の記憶手段と、

前記所定の入出力手順に従った前記機密データの入出力に関するログ情報と入出力の対象となる前記機密データの前記第 1 の記憶手段における記憶位置を示すアドレスとを記憶する第 2 の記憶手段とを備えるデータ記憶装置。

【請求項 2】 前記機密データの入出力を制御する制御手段をさらに備え、前記ログ情報は、

入出力の対象となる前記機密データを識別する識別コードと、

入出力の対象となる前記機密データの前記第 1 の記憶手段における記憶状態を示す第 1 のステータスとを含み、

前記制御手段は、前記所定の入出力手順に従って、入出力の対象となる前記機密データの前記識別コードと前記アドレスとを前記インターフェース手段を介して受取ると前記第 2 の記憶手段に記憶し、前記インターフェース手段を介して受ける外部からの要求に応じて、前記第 2 の記憶手段に記憶された前記識別コードと前記アドレスとに基づいて前記第 1 の記憶手段における前記機密データの記憶状態を確認し、前記記憶状態に基づいて前記第 1 のステータスを更新する、請求項 1 に記載のデータ記憶装置。

【請求項 3】 前記ログ情報は、入出力の対象となった前記機密データの入出力における前記所定の入出力手順の進行状態を記録する第 2 のステータスをさらに含み、

前記制御手段は、前記所定の入出力手順の進行に応じて前記第 2 のステータスを更新する、請求項 2 に記載のデータ記憶装置。

【請求項 4】 前記ログ情報は、前記所定の入出力手順を特定する手順特定

情報をさらに含み、

前記制御手段は、前記手順特定情報を新たに取得するごとに前記手順特定情報を更新する、請求項2または請求項3に記載のデータ記憶装置。

【請求項5】 前記機密データは、その機密データに固有の前記識別コードを含み、

前記制御手段は、前記第1の記憶手段における前記機密データの記憶状態を確認するとき、前記アドレスによって特定される前記第1の記憶手段上の記憶位置に記憶されている前記機密データに含まれる前記識別コードによって前記機密データを特定する、請求項2から請求項4のいずれか1項に記載のデータ記憶装置。

【請求項6】 前記機密データを前記インターフェース手段を介して受取って前記第1の記憶手段に記憶する入力手順において、

前記制御手段は、前記受取った機密データに含まれる識別コードと前記ログ情報に含まれる識別コードとが一致しないとき、前記機密データを前記第1の記憶手段に記憶することなく、前記入力手順を中止する、請求項5に記載のデータ記憶装置。

【請求項7】 前記第1の記憶手段に記憶された前記機密データを前記インターフェース手段を介して出力する出力手順において、

前記制御手段は、前記アドレスによって特定される前記第1の記憶手段上の記憶位置に記憶されている前記機密データに含まれる識別コードと前記ログ情報に含まれる識別コードとが一致しないとき、前記機密データの出力を行なうことなく、前記出力手順を中止する、請求項5または請求項6に記載のデータ記憶装置。

【請求項8】 前記ログ情報に対する署名データを生成し、前記生成した署名データを前記ログ情報に添付した署名付きログ情報を生成する署名手段をさらに備え、

前記機密データを前記インターフェース手段を介して受取って前記第1の記憶手段に記憶する入力手順が中断した場合、中断した前記入力手順を再開する再入力手順において、

前記制御手段は、前記署名手段によって生成された前記署名付きログ情報を前記インターフェース手段を介して出力する、請求項2から請求項7のいずれか1項に記載のデータ記憶装置。

【請求項9】 前記インターフェース手段を介して前記機密データの提供先から受取った、前記提供先のもう1つのログ情報に対する署名データが前記もう1つのログ情報に添付されたもう1つの署名付きログ情報の正当性を検証して認証するログ認証手段をさらに備え、

前記第1の記憶手段に記憶された前記機密データを前記インターフェース手段を介して出力する出力手順が中断した場合、中断した前記出力手順を再開する再出力手順において、

前記ログ認証手段は、前記中断した出力手順における前記機密データの提供先から受取った前記もう1つの署名付きログ情報の正当性を検証し、

前記制御手段は、前記もう1つの署名付きログ情報が正当でないと判断されたとき、または、前記もう1つの署名付きログ情報が正当であると認証され、かつ、前記もう1つの署名付きログ情報と前記第2の記憶手段に記憶される前記ログ情報とに基づいて前記出力手順が中断していないと判断したとき、前記再出力手順を中止する、請求項8に記載のデータ記憶装置。

【請求項10】 前記機密データの提供元に対して出力する証明書を保持する証明書保持手段をさらに備え、

前記制御手段は、前記機密データを前記インターフェース手段を介して受取って前記第1の記憶手段に記憶する入力手順を開始するに際し、前記インターフェース手段を介して受取った前記証明書の出力要求に応じて前記証明書を前記インターフェース手段を介して出力し、前記提供元において前記証明書が認証されると、前記提供元から前記インターフェース手段を介して前記機密データを受取る、請求項4に記載のデータ記憶装置。

【請求項11】 前記証明書は、当該データ記憶装置に対応した公開鍵を含み、

前記公開鍵により暗号化されたデータを復号するための秘密鍵を保持する秘密鍵保持手段と、

前記公開鍵により暗号化されたデータを前記秘密鍵により復号する第 1 の復号処理手段と、

前記機密データを入出力する前記所定の入出力手順において、前記所定の入出力手順ごとに固有の第 1 のセッション鍵を生成するセッション鍵生成手段と、

前記提供元において生成された第 2 のセッション鍵によりデータを暗号化する暗号処理手段と、

前記第 1 のセッション鍵により暗号化されたデータを復号する第 2 の復号処理手段とをさらに備え、

前記入力手順において、

前記セッション鍵生成手段は、前記第 1 のセッション鍵を生成し、

前記第 1 の復号処理手段は、前記公開鍵により暗号化された前記第 2 のセッション鍵を前記秘密鍵により復号し、

前記暗号処理手段は、前記第 1 の復号処理手段から受けた前記第 2 のセッション鍵により前記第 1 のセッション鍵を暗号化し、

前記第 2 の復号処理手段は、前記第 1 のセッション鍵により暗号化された前記機密データを前記第 1 のセッション鍵により復号し、

前記制御手段は、前記提供元から前記インターフェース手段を介して受取った前記公開鍵によって暗号化された前記第 2 のセッション鍵を前記第 1 の復号処理手段に与え、前記第 2 のセッション鍵により暗号化された前記第 1 のセッション鍵を前記インターフェース手段を介して前記提供元に対して提供するために出力し、前記提供元から前記インターフェース手段を介して受取った前記第 1 のセッション鍵により暗号化された前記機密データを前記第 2 の復号処理手段に与え、復号された前記機密データを前記アドレスによって特定される前記第 1 の記憶手段上の記憶位置に記憶する、請求項 10 に記載のデータ記憶装置。

【請求項 12】 前記手順特定情報は、前記入力手順を特定する前記第 1 のセッション鍵であり、

前記制御手段は、前記セッション鍵生成手段によって前記第 1 のセッション鍵が生成されるごとに前記手順特定情報を更新する、請求項 11 に記載のデータ記憶装置。

【請求項13】 前記第1の復号処理手段から受けた前記第2のセッション鍵によって認証可能な前記ログ情報に対する署名データを生成し、前記生成した署名データを前記ログ情報に添付した署名付きログ情報を生成する署名手段をさらに備え、

前記入力手順が中断した場合に前記入力手順を再開する再入力手順において、

前記第1の復号処理手段は、新たに前記提供元から前記インターフェース手段を介して受取った前記公開鍵によって暗号化された前記第2のセッション鍵を復号し、

前記署名手段は、前記第2の記憶手段に記憶される前記第1のステータスが更新された後、新たに受取られた前記第2のセッション鍵によって前記署名付きログ情報を生成し、

前記制御手段は、新たに前記提供元から前記インターフェース手段を介して受取った前記公開鍵によって暗号化された前記第2のセッション鍵を前記第1の復号処理手段に与え、前記第1のステータスを更新し、前記署名手段によって生成された前記署名付きログ情報を前記インターフェース手段を介して前記提供元に対して提供するために出力する、請求項11または請求項12に記載のデータ記憶装置。

【請求項14】 前記機密データは、その機密データに固有の前記識別コードを含み、

前記制御手段は、前記第1の記憶手段における前記機密データの記憶状態を確認するとき、前記アドレスによって特定される前記第1の記憶手段上の記憶位置に記憶されている前記機密データに含まれる前記識別コードによって前記機密データを特定する、請求項10から請求項13のいずれか1項に記載のデータ記憶装置。

【請求項15】 前記制御手段は、前記受取った機密データに含まれる識別コードと前記ログ情報に含まれる識別コードとが一致しないとき、前記機密データの前記第1の記憶手段への記憶を中止する、請求項14に記載のデータ記憶装置。

【請求項16】 前記第1の記憶手段に記憶された前記機密データを提供す

る提供先から受取った、前記提供先のもう1つの証明書の正当性を検証して認証する認証手段をさらに備え、

前記機密データを前記インターフェース手段を介して出力する出力手順において、

前記認証手段は、前記提供先から受取った前記もう1つの証明書を検証し、

前記制御手段は、前記提供先から前記インターフェース手段を介して受取った前記もう1つの証明書を前記認証手段に与え、前記認証手段によって前記もう1つの証明書が認証されないとき、前記出力手順を中止する、請求項10に記載のデータ記憶装置。

【請求項17】 前記第1の記憶手段に記憶された前記機密データを提供する提供先から受取った、前記提供先のもう1つの証明書の正当性を検証して認証する認証手段と、

前記もう1つの証明書に含まれる前記提供先に対応した公開鍵によってデータを暗号化するもう1つの暗号処理手段とをさらに備え、

前記機密データを前記インターフェース手段を介して出力する出力手順において、

前記認証手段は、前記提供先から受取った前記もう1つの証明書を検証し、

前記セッション鍵生成手段は、第3のセッション鍵をさらに生成し、

前記もう1つの暗号処理手段は、前記提供先に対応した公開鍵により前記第3のセッション鍵を暗号化し、

前記第2の復号処理手段は、前記第3のセッション鍵により暗号化された前記提供先において生成された第4のセッション鍵を前記第3のセッション鍵によりさらに復号し、

前記暗号処理手段は、前記第2の復号処理手段から受けた前記第4のセッション鍵により前記機密データをさらに暗号化し、

前記制御手段は、前記提供先から前記インターフェース手段を介して受取った前記もう1つの証明書を前記認証手段に与え、前記認証手段によって前記もう1つの証明書が認証されたとき、前記もう1つの証明書に含まれる前記提供先に対応した公開鍵を前記もう1つの暗号処理手段に与え、前記提供先に対応した公開

鍵により暗号化された前記第 3 のセッション鍵を前記インターフェース手段を介して前記提供先に対して提供するために出力し、前記提供先から前記インターフェース手段を介して受取った前記第 3 のセッション鍵により暗号化された前記第 4 のセッション鍵を前記第 2 の復号処理手段に与え、前記アドレスによって特定される前記第 1 の記憶手段上の記憶位置に記憶される前記機密データを取得して前記暗号処理手段に与え、前記第 4 のセッション鍵により暗号化された前記機密データを前記インターフェース手段を介して前記提供先に対して提供するために出力する、請求項 1 1 から請求項 1 3 のいずれか 1 項に記載のデータ記憶装置。

【請求項 1 8】 前記手順特定情報は、前記出力手順を特定する前記第 4 のセッション鍵であり、

前記制御手段は、前記第 2 の復号処理手段によって前記第 3 のセッション鍵により暗号化された前記第 4 のセッション鍵が復号されるごとに前記手順特定情報を更新する、請求項 1 7 に記載のデータ記憶装置。

【請求項 1 9】 前記機密データは、その機密データに固有の前記識別コードを含み、

前記制御手段は、前記アドレスによって特定される前記第 1 の記憶手段上の記憶位置に記憶されている前記機密データに含まれる前記識別コードと前記ログ情報に含まれる識別コードとが一致しないとき、前記機密データの出力を行なうことなく、前記出力手順を中止する、請求項 1 6 から請求項 1 8 のいずれか 1 項に記載のデータ記憶装置。

【請求項 2 0】 前記インターフェース手段を介して前記機密データの提供先から受取った、前記提供先のもう 1 つのログ情報に対する署名データが前記もう 1 つのログ情報に添付された署名付きログ情報の正当性を検証して認証するログ認証手段をさらに備え、

前記第 1 の記憶手段に記憶された前記機密データを前記インターフェース手段を介して出力する出力手順が中断した場合、中断した前記出力手順を再開する再出力手順において、

前記ログ認証手段は、前記中断した出力手順における前記機密データの提供先から受取った前記署名付きログ情報の正当性を検証し、

前記制御手段は、前記署名付きログ情報が正当でないと判断されたとき、または、前記署名付きログ情報が正当であると認証され、かつ、前記署名付きログ情報と当該データ記憶装置の前記第2の記憶手段に記憶される前記ログ情報とに基づいて前記出力手順が中断していないと判断したとき、前記再出力手順を中止する、請求項16に記載のデータ記憶装置。

【請求項21】 前記インターフェース手段を介して前記機密データの提供先から受取った、前記第4のセッション鍵によって前記提供先のもう1つのログ情報に署名されたもう1つの署名付きログ情報の正当性を検証して認証するログ認証手段をさらに備え、

前記第1の記憶手段に記憶された前記機密データを前記インターフェース手段を介して出力する出力手順が中断した場合、中断した前記出力手順を再開する再出力手順において、

前記ログ認証手段は、前記中断した出力手順における前記機密データの提供先から受取った前記もう1つの署名付きログ情報の正当性を検証し、

前記制御手段は、前記もう1つの署名付きログ情報が正当でないと判断されたとき、または、前記もう1つの署名付きログ情報が正当であると認証され、かつ、前記もう1つの署名付きログ情報と当該データ記憶装置の前記第2の記憶手段に記憶される前記ログ情報とに基づいて前記出力手順が中断していないと判断したとき、前記再出力手順を中止する、請求項17または請求項18に記載のデータ記憶装置。

【請求項22】 前記機密データは、暗号化されたコンテンツデータを復号して利用するための復号鍵であって、

前記暗号化されたコンテンツデータを記憶するための第3の記憶手段をさらに備える、請求項1から請求項21のいずれか1項に記載のデータ記憶装置。

【請求項23】 前記第3の記憶手段は、ハードディスクである、請求項22に記載のデータ記憶装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、デジタルデータ化されたコンテンツデータに対する著作権保護を可能とするデータ配信システムにおけるデータ記憶装置に関し、特に、コンテンツデータを暗号化した暗号化コンテンツデータの再生に際して必要とされるライセンス（復号鍵および利用規則）を安全に入出力し、かつ、多数のライセンスを記憶することができ、さらには、保護を必要とする機密データを安全に入出力し、かつ、機密データの入出力の中断から安全に入出力を再開できるデータ記憶装置に関する。

【0002】

【従来の技術】

近年、インターネット等のデジタル情報通信網等の進歩により、個人端末から各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【0003】

このようなデジタル情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【0004】

したがって、このようなデジタル情報通信網上において音楽データや画像データ等の著作権者の権利が存在するコンテンツが伝送される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【0005】

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介してコンテンツの配信を行なうことができないとすると、基本的には、コンテンツデータの複製に際して一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【0006】

ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデ

ータを記録した記録媒体を例にとって考えてみると、通常販売されている音楽データを記録したCD（コンパクトディスク）については、CDから光磁気ディスク（MD等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して補償金として支払うことになっている。

【0007】

しかも、CDからMDへ音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なMDからさらに他のMDに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【0008】

このような事情からも、音楽データや画像データ等のコンテンツデータをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【0009】

同様に、デジタル情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【0010】

そこで、デジタル情報通信網を介したデータ配信システムとして、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバから携帯電話機などの端末装置に装着されたデータ記憶装置としてのメモリカードに対して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書とを暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、認証された証明書を配信サーバが受信したことを確認した上で、暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのコンテンツ鍵とをメ

メモリカードに対して送信する。そして、暗号化コンテンツデータやコンテンツ鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッション鍵を発生させ、その発生させたセッション鍵によって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【0011】

最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッション鍵によって暗号化したライセンスと、暗号化コンテンツデータとをメモリカードへ送信する。そして、メモリカードは、受信したコンテンツ鍵と暗号化コンテンツデータとをメモリに記憶する。

【0012】

そして、ユーザは、メモリカードに記憶した暗号化コンテンツデータを再生するときは、メモリカードを専用の再生回路を備えた再生端末に接続し、その暗号化コンテンツデータを再生して楽しむことができる。

【0013】

このようなシステムにおいて、コンテンツ供給者あるいは著作権者によって暗号化コンテンツデータの再生や複製に関する利用方法が指示できるように利用規則を定め、この利用規則をコンテンツ鍵とともに配信し、各機器が利用規則に従って処理を行なうことができるようになっている。

【0014】

利用規則には、メモリカード間のライセンスの複製・移動に関する規則、再生回数の制限などのコンテンツ鍵をメモリカードから出力する場合の規制や、再生されたコンテンツの取扱いに関する規則が規定されている。

【0015】

【発明が解決しようとする課題】

上述したようなデータ配信システムにおいては、暗号化コンテンツデータと、暗号化コンテンツデータの復号および利用に関するライセンスとが、配信サーバとデータ記憶装置との間や、あるいはデータ記憶装置と再生端末との間などで送受信される。ここで、ライセンスとは、暗号化コンテンツデータを復号するためのコンテンツ鍵や、コンテンツに対するライセンスを特定するためのライセンス

ID、あるいは上述したコンテンツの利用規則などを総称するものである。そして、このライセンスこそが著作権を保護する目的からセキュリティに十分配慮して送受信されるべきものである。

【0016】

ここで、ライセンスを装置間で送受信する際に、通常の送受信処理中であれば、送信側と受信側とにおいて送受信を行なっているライセンスを互いに認識し、ライセンスは両装置の間を問題なく送受信されるが、ライセンスの送受信中にいずれかの装置あるいは通信路において異常（たとえば、装置の電源の遮断など）が発生すると、送受信中のライセンスが消失してしまうことがある。

【0017】

たとえば、データ記憶装置間でライセンスの送受信を行なう場合、利用規則によってライセンスの複製が許可されているフリーなコンテンツを除いては、著作権保護の観点から、送信側のデータ記憶装置および受信側のデータ記憶装置の両装置において同時に同一のライセンスが利用可能な状態で記憶できない構成となっている。すなわち、送信側のデータ記憶装置に記憶されているライセンスは、受信側のデータ記憶装置に対してライセンスを出力すると同時に利用できないものとなる必要がある。このような場合、一時的にはあるが、両データ記憶装置のいずれにも利用できるライセンスが記憶されていない状態が発生する。このような場合において、異常が発生して送受信処理が中断すると、送信中のライセンスが消失してしまうのである。配信サーバからライセンスを受信する場合においても、同様にライセンスの消失の危険性がある。したがって、ライセンスの送受信が中断した場合に、中断した送受信処理およびライセンスを特定し、特定したライセンスの記憶状態を把握したうえで、ライセンスの消失が発生した場合には、消失したライセンスの再送信処理をいかに適切に行なうかが重要になってくる。そして、データ記憶装置には、送受信中であった送受信処理とライセンスとを再度特定するための情報を効率的に記録しておく必要がある。

【0018】

一方、近年、そして今後さらなる飛躍的進歩が確実視されるIT技術の進展に伴う情報量の増大、情報のマルチメディア化、通信技術の高度化、また、メモリ

技術の進展に伴うデータ記憶装置の大容量化などとあいまって、上述したデータ配信システムにおけるデータ記憶装置には、多種多様、かつ、相当数のコンテンツデータが記憶されるものと予想される。

【0019】

この場合、大容量のデータ記憶装置において相当数のコンテンツデータを記憶し、それに伴って各々のコンテンツデータに対応するライセンスを保持している場合において、上述したデータ配信システムにおいてライセンスの送受信処理中に異常が発生したときに、送受信中のライセンスを相当数記憶されたライセンスの中から再度特定することは、記憶されるライセンスの数が増えるほど、その検索に時間がかかることになる。

【0020】

従来のシステムにおいては、このような場合、全てのライセンスを逐一検索して特定するしかなく、検索に要する処理時間が問題とされていた。

【0021】

そこで、この発明は、かかる課題を解決するためになされたものであり、その目的は、相当数記憶されたライセンスの中から送受信処理中のライセンスを迅速に特定でき、特にライセンスの送受信処理中に異常が発生したときに、ライセンスの保護と再処理の高速化とを両立するデータ記憶装置を提供することである。

【0022】

【課題を解決するための手段】

この発明によれば、データ記憶装置は、機密データを保護するための所定の入出力手順に従って機密データの入出力を行ない、かつ、機密データを記憶するデータ記憶装置であって、外部とデータのやり取りを行なうインターフェース手段と、機密データを記憶する第1の記憶手段と、所定の入出力手順に従った機密データの入出力に関するログ情報と入出力の対象となる機密データの第1の記憶手段における記憶位置を示すアドレスとを記憶する第2の記憶手段とを備える。

【0023】

好ましくは、データ記憶装置は、機密データの入出力を制御する制御手段をさらに備え、ログ情報は、入出力の対象となる機密データを識別する識別コードと

、入出力の対象となる機密データの第1の記憶手段における記憶状態を示す第1のステータスとを含み、制御手段は、所定の入出力手順に従って、入出力の対象となる機密データの識別コードとアドレスとをインターフェース手段を介して受取ると第2の記憶手段に記憶し、インターフェース手段を介して受ける外部からの要求に応じて、第2の記憶手段に記憶された識別コードとアドレスとに基づいて第1の記憶手段における機密データの記憶状態を確認し、記憶状態に基づいて第1のステータスを更新する。

【0024】

好ましくは、ログ情報は、入出力の対象となった機密データの入出力における所定の入出力手順の進行状態を記録する第2のステータスをさらに含み、制御手段は、所定の入出力手順の進行に応じて第2のステータスを更新する。

【0025】

好ましくは、ログ情報は、所定の入出力手順を特定する手順特定情報をさらに含み、制御手段は、手順特定情報を新たに取得することに手順特定情報を更新する。

【0026】

好ましくは、機密データは、その機密データに固有の識別コードを含み、制御手段は、第1の記憶手段における機密データの記憶状態を確認するとき、アドレスによって特定される第1の記憶手段上の記憶位置に記憶されている機密データに含まれる識別コードによって機密データを特定する。

【0027】

好ましくは、機密データをインターフェース手段を介して受取って第1の記憶手段に記憶する入力手順において、制御手段は、受取った機密データに含まれる識別コードとログ情報に含まれる識別コードとが一致しないとき、機密データを第1の記憶手段に記憶することなく、入力手順を中止する。

【0028】

好ましくは、第1の記憶手段に記憶された機密データをインターフェース手段を介して出力する出力手順において、制御手段は、アドレスによって特定される第1の記憶手段上の記憶位置に記憶されている機密データに含まれる識別コード

とログ情報に含まれる識別コードとが一致しないとき、機密データの出力を行なうことなく、出力手順を中止する。

【0029】

好ましくは、データ記憶装置は、ログ情報に対する署名データを生成し、生成した署名データをログ情報に添付した署名付きログ情報を生成する署名手段をさらに備え、機密データをインターフェース手段を介して受取って第1の記憶手段に記憶する入力手順が中断した場合、中断した入力手順を再開する再入力手順において、制御手段は、署名手段によって生成された署名付きログ情報をインターフェース手段を介して出力する。

【0030】

好ましくは、データ記憶装置は、インターフェース手段を介して機密データの提供先から受取った、提供先のログ情報に対する署名データが提供先のログ情報に添付されたもう1つの署名付きログ情報の正当性を検証して認証するログ認証手段をさらに備え、第1の記憶手段に記憶された機密データをインターフェース手段を介して出力する出力手順が中断した場合、中断した出力手順を再開する再出力手順において、ログ認証手段は、中断した出力手順における機密データの提供先から受取ったもう1つの署名付きログ情報の正当性を検証し、制御手段は、もう1つの署名付きログ情報が正当でないと判断されたとき、または、もう1つの署名付きログ情報が正当であると認証され、かつ、もう1つの署名付きログ情報と第2の記憶手段に記憶される当該データ記憶装置のログ情報とに基づいて出力手順が中断していないと判断したとき、再出力手順を中止する。

【0031】

好ましくは、データ記憶装置は、機密データの提供元に対して出力する証明書を保持する証明書保持手段をさらに備え、制御手段は、機密データをインターフェース手段を介して受取って第1の記憶手段に記憶する入力手順を開始するに際し、インターフェース手段を介して受取った証明書の出力要求に応じて証明書をインターフェース手段を介して出力し、提供元において証明書が認証されると、提供元からインターフェース手段を介して機密データを受取る。

【0032】

好ましくは、証明書は、当該データ記憶装置に対応した公開鍵を含み、公開鍵により暗号化されたデータを復号するための秘密鍵を保持する秘密鍵保持手段と、公開鍵により暗号化されたデータを秘密鍵により復号する第1の復号処理手段と、機密データを入出力する所定の入出力手順において、所定の入出力手順ごとに固有の第1のセッション鍵を生成するセッション鍵生成手段と、提供元において生成された第2のセッション鍵によりデータを暗号化する暗号処理手段と、第1のセッション鍵により暗号化されたデータを復号する第2の復号処理手段とをさらに備え、入力手順において、セッション鍵生成手段は、第1のセッション鍵を生成し、第1の復号処理手段は、公開鍵により暗号化された第2のセッション鍵を秘密鍵により復号し、暗号処理手段は、第1の復号処理手段から受けた第2のセッション鍵により第1のセッション鍵を暗号化し、第2の復号処理手段は、第1のセッション鍵により暗号化された機密データを第1のセッション鍵により復号し、制御手段は、提供元からインターフェース手段を介して受取った公開鍵によって暗号化された第2のセッション鍵を第1の復号処理手段に与え、第2のセッション鍵により暗号化された第1のセッション鍵をインターフェース手段を介して提供元に対して提供するために出力し、提供元からインターフェース手段を介して受取った第1のセッション鍵により暗号化された機密データを第2の復号処理手段に与え、復号された機密データをアドレスによって特定される第1の記憶手段上の記憶位置に記憶する。

【0033】

好ましくは、手順特定情報は、入力手順を特定する第1のセッション鍵であり、制御手段は、セッション鍵生成手段によって第1のセッション鍵が生成されるごとに手順特定情報を更新する。

【0034】

好ましくは、データ記憶装置は、第1の復号処理手段から受けた第2のセッション鍵によって認証可能なログ情報に対する署名データを生成し、生成した署名データをログ情報に添付した署名付きログ情報を生成する署名手段をさらに備え、入力手順が中断した場合に入力手順を再開する再入力手順において、第1の復号処理手段は、新たに提供元からインターフェース手段を介して受取った公開鍵

によって暗号化された第2のセッション鍵を復号し、署名手段は、第2の記憶手段に記憶される第1のステータスが更新された後、新たに受取られた第2のセッション鍵によって署名付きログ情報を生成し、制御手段は、新たに提供元からインターフェース手段を介して受取った公開鍵によって暗号化された第2のセッション鍵を第1の復号処理手段に与え、第1のステータスを更新し、署名手段によって生成された署名付きログ情報をインターフェース手段を介して提供元に対して提供するために出力する。

【0035】

好ましくは、機密データは、その機密データに固有の識別コードを含み、制御手段は、第1の記憶手段における機密データの記憶状態を確認するとき、アドレスによって特定される第1の記憶手段上の記憶位置に記憶されている機密データに含まれる識別コードによって機密データを特定する。

【0036】

好ましくは、制御手段は、受取った機密データに含まれる識別コードとログ情報に含まれる識別コードとが一致しないとき、機密データの第1の記憶手段への記憶を中止する。

【0037】

好ましくは、データ記憶装置は、第1の記憶手段に記憶された機密データを提供する提供先から受取った、提供先のもう1つの証明書の正当性を検証して認証する認証手段をさらに備え、機密データをインターフェース手段を介して出力する出力手順において、認証手段は、提供先から受取ったもう1つの証明書を検証し、制御手段は、提供先からインターフェース手段を介して受取ったもう1つの証明書を認証手段に与え、認証手段によってもう1つの証明書が認証されないとき、出力手順を中止する。

【0038】

好ましくは、データ記憶装置は、第1の記憶手段に記憶された機密データを提供する提供先から受取った、提供先のもう1つの証明書の正当性を検証して認証する認証手段と、もう1つの証明書に含まれる提供先に対応した公開鍵によってデータを暗号化するもう1つの暗号処理手段とをさらに備え、機密データをイン

ターフェース手段を介して出力する出力手順において、認証手段は、提供先から受取ったもう1つの証明書を検証し、セッション鍵生成手段は、第3のセッション鍵をさらに生成し、もう1つの暗号処理手段は、提供先に対応した公開鍵により第3のセッション鍵を暗号化し、第2の復号処理手段は、第3のセッション鍵により暗号化された提供先において生成された第4のセッション鍵を第3のセッション鍵によりさらに復号し、暗号処理手段は、第2の復号処理手段から受けた第4のセッション鍵により機密データをさらに暗号化し、制御手段は、提供先からインターフェース手段を介して受取ったもう1つの証明書を認証手段に与え、認証手段によってもう1つの証明書が認証されたとき、もう1つの証明書に含まれる提供先に対応した公開鍵をもう1つの暗号処理手段に与え、提供先に対応した公開鍵により暗号化された第3のセッション鍵をインターフェース手段を介して提供先に対して提供するために出力し、提供先からインターフェース手段を介して受取った第3のセッション鍵により暗号化された第4のセッション鍵を第2の復号処理手段に与え、アドレスによって特定される第1の記憶手段上の記憶位置に記憶される機密データを取得して暗号処理手段に与え、第4のセッション鍵により暗号化された機密データをインターフェース手段を介して提供先に対して提供するために出力する。

【0039】

好ましくは、手順特定情報は、出力手順を特定する第4のセッション鍵であり、制御手段は、第2の復号処理手段によって第3のセッション鍵により暗号化された第4のセッション鍵が復号されるごとに手順特定情報を更新する。

【0040】

好ましくは、機密データは、その機密データに固有の識別コードを含み、制御手段は、アドレスによって特定される第1の記憶手段上の記憶位置に記憶されている機密データに含まれる識別コードとログ情報に含まれる識別コードとが一致しないとき、機密データの出力を行なうことなく、出力手順を中止する。

【0041】

好ましくは、データ記憶装置は、インターフェース手段を介して機密データの提供先から受取った、提供先のログ情報に対する署名データが提供先のログ情報

に添付された署名付きログ情報の正当性を検証して認証するログ認証手段をさらに備え、第1の記憶手段に記憶された機密データをインターフェース手段を介して出力する出力手順が中断した場合、中断した出力手順を再開する再出力手順において、ログ認証手段は、中断した出力手順における機密データの提供先から受取った署名付きログ情報の正当性を検証し、制御手段は、署名付きログ情報が正当でないと判断されたとき、または、署名付きログ情報が正当であると認証され、かつ、署名付きログ情報と当該データ記憶装置の第2の記憶手段に記憶される当該データ記憶装置のログ情報とに基づいて出力手順が中断していないと判断したとき、再出力手順を中止する。

【0042】

好ましくは、データ記憶装置は、インターフェース手段を介して機密データの提供先から受取った、第4のセッション鍵によって提供先のログ情報に署名されたもう1つの署名付きログ情報の正当性を検証して認証するログ認証手段をさらに備え、第1の記憶手段に記憶された機密データをインターフェース手段を介して出力する出力手順が中断した場合、中断した出力手順を再開する再出力手順において、ログ認証手段は、中断した出力手順における機密データの提供先から受取ったもう1つの署名付きログ情報の正当性を検証し、制御手段は、もう1つの署名付きログ情報が正当でないと判断されたとき、または、もう1つの署名付きログ情報が正当であると認証され、かつ、もう1つの署名付きログ情報と当該データ記憶装置の第2の記憶手段に記憶される当該データ記憶装置のログ情報とに基づいて出力手順が中断していないと判断したとき、再出力手順を中止する。

【0043】

好ましくは、機密データは、暗号化されたコンテンツデータを復号して利用するための復号鍵であって、暗号化されたコンテンツデータを記憶するための第3の記憶手段をさらに備える。

【0044】

好ましくは、第3の記憶手段は、ハードディスクである。

【0045】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【0046】

〔実施の形態1〕

図1は、本発明によるデータ記憶装置が、暗号化コンテンツデータおよび暗号化コンテンツデータを復号するためのライセンスを取得するデータ配信システムの全体構成を概念的に説明するための概略図である。

【0047】

なお、以下では、デジタル放送網により配信された映像データを端末装置10により受信して端末装置10に装着されたデータ記憶装置であるHD（ハードディスク）20に記憶し、また、暗号化された映像データを復号するためのライセンスを双方向のネットワーク30に接続される端末装置10によりネットワーク30を介してライセンス提供装置40から受信してHD20に格納し、暗号化された映像データを端末装置10に内蔵された専用の再生回路（図示せず）にて再生するデータ配信システムの構成を例にとって説明する。一方、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、音楽データ、教材データ、朗読データ、書籍データ、ゲームなどのプログラムが扱われる場合においても適用することが可能なものである。また、データ記憶装置についても同様に、ハードディスクに限定されることなく、他のデータ記憶装置、たとえばメモリカードなどにおいても適用することが可能である。

【0048】

図1を参照して、端末装置10は、デジタル放送網により配信される、暗号化された映像データ（以下、コンテンツデータとも呼ぶ）をアンテナ11を介して受信し、HD20に記憶する。暗号化されたコンテンツデータを復号するためのコンテンツ鍵を含むライセンスを管理し配信するライセンス提供装置40は、ライセンスの配信を求めてアクセスしてきた端末装置10に装着されたHD20が正当な認証データを持つか否か、すなわち、ライセンス管理機能を備えた正規のデータ記憶装置であるか否かの認証処理を行ない、HD20が正当なデータ記憶

装置であった場合のみ、端末装置 1 0 に対して H D 2 0 においてのみ復号可能な所定の暗号方式によって暗号化したライセンスを送信する。そして、端末装置 1 0 は、ネットワーク 3 0 に接続されたモデムを介して暗号化されたライセンスを受信すると、その暗号化されたライセンスを装着された H D 2 0 へ送信する。

【 0 0 4 9 】

図 1 においては、たとえば、H D 2 0 は、端末装置 1 0 に着脱可能な構成となっている。端末装置 1 0 に装着された H D 2 0 は、端末装置 1 0 により受信された暗号化されたライセンスを受取り、著作権を保護するためにライセンス対してなされている暗号化を復号したうえで H D 2 0 内に記憶する。そして、ライセンスに対応した暗号化コンテンツデータを再生する場合、ライセンスに含まれるコンテンツ鍵と暗号化コンテンツデータとを端末装置 1 0 に与える。

【 0 0 5 0 】

そして、端末装置 1 0 のユーザは、端末装置 1 0 においてコンテンツ鍵を用いて復号されるコンテンツデータを再生することが可能となる。

【 0 0 5 1 】

このような構成とすることで、端末装置 1 0 のユーザは、ライセンス管理機能を備え、正規な認証データを有する H D 2 0 を利用しないと、暗号化されたコンテンツデータを受信して記憶したところでライセンスの提供を受けることができず、コンテンツデータを再生することができない。

【 0 0 5 2 】

なお、上述したデータ配信システムにおいては、暗号化コンテンツデータの提供元は、デジタル放送業者の放送サーバであるが、コンテンツのライセンスを管理するライセンス提供装置 4 0 であってもよいし、インターネットなどの通信網を介して接続されるライセンス提供装置 4 0 とは別の配信サーバであってもよく、また、他のユーザからの複製であってもよい。すなわち、暗号化コンテンツデータ自体は、どこから発信されても、また、どこで受信されてもよく、要は暗号化コンテンツデータを復号可能なライセンスを厳重に管理しておきさえすれば、コンテンツデータの著作権を保護することができる。

【 0 0 5 3 】

したがって、本発明の実施の形態においては、HD 20、端末装置10およびライセンス提供装置40のそれぞれの間で行なわれるライセンスの送受信処理において、暗号化コンテンツデータを再生するために必要なライセンスの提供元が、提供先に対する認証およびチェック機能を行ない、非認証の装置に対するライセンスの出力を防止する。さらに、ライセンスの送受信処理中に異常が発生したときに、ライセンスが重複して存在することがないように、再処理の必要なライセンスを特定することでコンテンツデータの著作権保護を実現しつつ、不慮の送受信処理の異常終了から回復可能なシステムの構成について説明する。

【0054】

図2は、図1に示したデータ配信システムにおいて送受信されるデータ、情報等の特性を説明する図である。

【0055】

データDcは、コンテンツデータであって、ここでは映像データである。データDcは、コンテンツ鍵Kcで復号可能な暗号化が施される。コンテンツ鍵Kcによって復号可能な暗号化が施された暗号化コンテンツデータE(Kc, Dc)が、この形式でデジタル放送網により端末装置10のユーザに配布される。

【0056】

なお、以下においては、E(X, Y)という表記は、データYを、復号鍵Xにより復号可能な暗号化を施したことを示すものとする。また、データDcに付随して、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Diが配布される。

【0057】

また、ライセンスの配信を特定するとともに、各々のライセンスを特定する管理コードであるライセンスID(LID)が端末装置10を介してライセンス提供装置40とHD20との間でやり取りされる。さらに、ライセンスとしては、データDcおよびコンテンツ鍵Kcを識別するためのコードであるデータID(DID)や、利用者側からの指定によって決定されるライセンス数や機能限定など、データ記憶装置におけるライセンスや再生の取扱いに対する制限に関する制御情報ACが存在する。

【0058】

コンテンツ鍵 K_c と、制御情報 AC と、 DID と、 LID とを併せて、以後、ライセンス LIC と総称することとする。 DID は、データ D_c とコンテンツ鍵 K_c との対に対して割り当てられた識別情報、すなわち、暗号化データ $E(K_c, D_c)$ を識別するための識別情報となる。 DID は、ライセンス LIC の他に、暗号化データ $E(K_c, D_c)$ とともに常に扱われる付加情報 Di にも含まれ、参照できるようになっている。

【0059】

図3は、図1に示すデータ配信システムにおいて使用される認証のためのデータ、情報等の特性を説明する図である。

【0060】

HD20などのデータ記憶装置および端末装置10などに備えられる再生回路には、固有のクラス公開鍵 KP_{cmy} および KP_{cpy} がそれぞれ設けられ、クラス公開鍵 KP_{cmy} および KP_{cpy} は、データ記憶装置に固有のクラス秘密鍵 K_{cmy} および再生回路に固有のクラス秘密鍵 K_{cpy} によってそれぞれ復号可能である。これらクラス公開鍵およびクラス秘密鍵は、再生回路あるいはデータ記憶装置の種類ごとに異なる値を持ち、これらクラス公開鍵およびクラス秘密鍵を共有する単位をクラスと称する。記号「 y 」は、そのクラスを識別するための識別子を表わす。クラスは、製造会社や製品の種類、製造時のロット等によって異なる。

【0061】

また、データ記憶装置のクラス証明書として C_{my} が設けられ、再生回路のクラス証明書として C_{py} が設けられる。これらのクラス証明書は、データ記憶装置および再生回路のクラスごとに異なる情報を有する。

【0062】

データ記憶装置のクラス証明書 C_{my} は、 $KP_{cmy} // I_{cmy} // E(K_a, H(KP_{cmy} // I_{cmy}))$ の形式で出荷時にデータ記憶装置に記憶され、再生回路のクラス証明書 C_{py} は、 $KP_{cpy} // I_{cpy} // E(K_a, H(KP_{cpy} // I_{cpy}))$ の形式で出荷時に再生回路に記憶される。ここ

で、 $X//Y$ は、 X と Y との連結を表わし、 $H(X)$ は、ハッシュ関数により演算されたデータ X のハッシュ値を表わす。マスタ鍵 K_a は、これらのクラス証明書を作成するために使用される秘密暗号鍵であり、このデータ配信システム全体で共通の秘密暗号鍵であって、認証局によって安全に管理運用される。また、クラス情報 $I_{cm y}$ 、 $I_{cp y}$ は、クラスごとの機器に関する情報およびクラス公開鍵を含む情報データである。

【0063】

また、 $E(K_a, H(KP_{cm y} // I_{cm y}))$ および $E(K_a, H(KP_{cp y} // I_{cp y}))$ は、それぞれ $KP_{cm y} // I_{cm y}$ および $KP_{cp y} // I_{cp y}$ に対する電子署名を行なった署名データである。

【0064】

なお、認証局は、署名データを作成する公的機関であり、署名データ $E(K_a, H(KP_{cm y} // I_{cm y}))$ および $E(K_a, H(KP_{cp y} // I_{cp y}))$ は、認証局によって生成される。

【0065】

さらに、データ記憶装置に対して安全かつ確実にライセンスLICを送信するための鍵として、データ記憶装置という媒体ごとに設定される個別公開鍵 $KP_{om z}$ と、個別公開鍵 $KP_{om z}$ で暗号化されたデータを復号することが可能な個別秘密鍵 $K_{om z}$ とが存在する。ここで、記号「z」は、データ記憶装置を個別に識別するための識別子である。

【0066】

データ配信システムにおいてデータの送受信が行なわれるごとに、ライセンス提供装置40、データ記憶装置(HD20)、および端末装置10の再生回路において生成されるセッション鍵 $K_{s1 x}$ 、 $K_{s2 x}$ が用いられる。

【0067】

ここで、セッション鍵 $K_{s1 x}$ 、 $K_{s2 x}$ は、ライセンス提供装置40、データ記憶装置(HD20)、もしくは端末装置10の再生回路間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵である。

「セッション」には、ライセンス提供装置40からデータ記憶装置(HD20)

ヘライセンスを配信する「配信セッション」、データ記憶装置間でのライセンスの複製や移動を行なう「複製・移動セッション」、およびデータ記憶装置（HD 20）から端末装置10の再生回路ヘライセンスを出力する「再生許諾セッション」がある。

【0068】

これらのセッション鍵 $Ks1x$ 、 $Ks2x$ は、各セッションごとに固有の値を有することにより、ライセンス提供装置40、データ記憶装置（HD 20）、および端末装置10の再生回路によって管理される。具体的には、セッション鍵 $Ks1x$ は、ライセンスを送受信する際に、ライセンスの送信側によってセッションごとに発生され、セッション鍵 $Ks2x$ は、ライセンスの受信側によってセッションごとに発生される。なお、記号「x」は、セッションにおける一連の処理を識別するための識別子である。そして、各セッションにおいてこれらのセッション鍵を各機器間で相互に授受し、他の機器で生成されたセッション鍵を受けて、そのセッション鍵による暗号化を実行したうえで、ライセンスLIC、またはコンテンツ鍵を含むライセンスLICの一部の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【0069】

図4は、図1に示したライセンス提供装置40の構成を示す概略ブロック図である。

【0070】

ライセンス提供装置40は、管理対象のライセンスを保持するデータベースであるコンテンツDB402と、ライセンスを配信する配信セッションにおける一切の通信記録を記憶保持するデータベースであるログDB404と、コンテンツDB402およびログDB404とバスBS1を介してデータをやり取りし、所定の処理を行なうためのデータ処理部410と、ネットワーク30を介して端末装置10とデータ処理部410との間でデータ授受を行なうための通信装置450とを備える。

【0071】

データ処理部410は、バスBS1上のデータに応じて、データ処理部410

の動作を制御するための配信制御部412と、配信制御部412により制御されて、配信セッション時にセッション鍵 K_{s1x} を発生するためのセッション鍵発生部414と、端末装置10から送られてくるHD20のクラス証明書 C_{my} に含まれる署名データ $E(K_a, H(KP_{cmy} // I_{cmy}))$ を復号するためのHD20の認証鍵 KPa を保持する KPa 保持部416と、HD20から送られてきたクラス証明書 C_{my} を通信装置450およびバスBS1を介して受け、 KPa 保持部416から受ける認証鍵 KPa によって復号処理を行ない、クラス証明書 C_{my} に含まれる署名データ $E(K_a, H(KP_{cmy} // I_{cmy}))$ の復号処理と、クラス証明書 C_{my} に含まれる $KP_{cmy} // I_{cmy}$ のハッシュ値の計算を行ない、両者の結果を比較チェックしてクラス証明書 C_{my} の検証を行なう認証部418と、配信セッションごとに、セッション鍵発生部414により生成されたセッション鍵 K_{s1x} を認証部418によってクラス証明書 C_{my} から抽出したクラス公開鍵 KP_{cmy} を用いて暗号化し、バスBS1に出力するための暗号処理部420と、セッション鍵 K_{s1x} によって暗号化された上で送信されたデータをバスBS1より受け、復号処理を行なう復号処理部422とを含む。

【0072】

データ処理部410は、さらに、配信制御部412から与えられるライセンスLICを、復号処理部422によって得られたデータ記憶装置ごとに固有な個別公開鍵 KP_{omz} によって暗号化するための暗号処理部424と、暗号処理部424の出力を、復号処理部422から与えられるセッション鍵 K_{s2x} によってさらに暗号化してバスBS1に出力するための暗号処理部426とを含む。

【0073】

なお、個別公開鍵 KP_{omz} およびセッション鍵 K_{s2x} は、セッション鍵 K_{s1x} によって暗号化されたうえで端末装置10から提供される。復号処理部422は、これを復号して個別公開鍵 KP_{omz} を得る。

【0074】

ライセンス提供装置40の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【 0 0 7 5 】

図 5 は、図 1 に示した端末装置 1 0 の構成を説明するための概略ブロック図である。

【 0 0 7 6 】

端末装置 1 0 は、デジタル放送網によって伝送される信号を受信するアンテナ 1 0 2 と、アンテナ 1 0 2 からの信号を受けてベースバンド信号に変換、あるいはアンテナ 1 0 2 から送信するデータを変調してアンテナ 1 0 2 に与える受信部 1 0 4 と、端末装置 1 0 をネットワーク 3 0 に接続するモデム 1 0 6 と、端末装置 1 0 の各部のデータ授受を行なうバス B S 2 と、バス B S 2 を介して端末装置 1 0 の動作を制御するコントローラ 1 0 8 と、H D 2 0 とバス B S 2 との間のデータの授受を制御する H D インタフェース部 1 1 0 とを含む。

【 0 0 7 7 】

端末装置 1 0 は、さらに、上述したクラス証明書 C p y を保持する認証データ保持部 1 5 0 2 を含む。ここで、端末装置 1 0 のクラス y は、y = 3 であるとする。

【 0 0 7 8 】

端末装置 1 0 は、さらに、クラス固有の復号鍵であるクラス秘密鍵 K c p 3 を保持する K c p 保持部 1 5 0 4 と、バス B S 2 から受けたデータをクラス秘密鍵 K c p 3 によって復号し、H D 2 0 によって発生されたセッション鍵 K s 1 x を得る復号処理部 1 5 0 6 とを含む。

【 0 0 7 9 】

端末装置 1 0 は、さらに、H D 2 0 に記憶されたコンテンツデータの再生を行なう再生許諾セッションにおいて、H D 2 0 との間でやり取りされるデータを暗号化するためのセッション鍵 K s 2 x を乱数等により発生するセッション鍵発生部 1 5 0 8 と、H D 2 0 からコンテンツ鍵 K c を受取る際に、セッション鍵発生部 1 5 0 8 により発生されたセッション鍵 K s 2 x を復号処理部 1 5 0 6 によって得られたセッション鍵 K s 1 x によって暗号化し、バス B S 2 に出力する暗号処理部 1 5 1 0 と、バス B S 2 上のデータをセッション鍵 K s 2 x によって復号して、コンテンツ鍵 K c を出力する復号処理部 1 5 1 2 と、バス B S 2 より暗号

化コンテンツデータ $E(K_c, D_c)$ を受けて、復号処理部 1512 からのコンテンツ鍵 K_c によって暗号化コンテンツデータ $E(K_c, D_c)$ を復号してデータ D_c を再生部 1516 へ出力する復号処理部 1514 と、復号処理部 1514 からの出力を受けてコンテンツを再生するための再生部 1516 と、再生部 1516 の出力をデジタル信号からアナログ信号に変換する DA 変換部 1518 と、DA 変換部 1518 の出力をテレビモニターなどの外部出力装置（図示省略）へ出力するための端子 1520 とを含む。

【0080】

なお、図 5 においては、点線で囲んだ領域は暗号化コンテンツデータを復号して映像データを再生する専用回路である再生回路 150 を構成する。再生回路 150 は、セキュリティを向上させるために 1 チップ構成の半導体デバイスであることが好ましい。さらには、再生回路 150 は、外部からの解析が困難な耐タンパモジュールとして構成されることが好ましい。

【0081】

端末装置 10 の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0082】

図 6 は、図 1 に示す HD 20 の構成を説明するための概略ブロック図である。

すでに説明したように、ハードディスクのクラス公開鍵およびクラス秘密鍵として、 $K_{Pcm y}$ および $K_{cm y}$ が設けられ、ハードディスクのクラス証明書 $C_{m y}$ が設けられるが、HD 20 においては、自然数 $y = 1$ で表わされるものとする。また、HD 20 を識別する自然数 z は $z = 2$ で表されるものとする。

【0083】

したがって、HD 20 は、クラス証明書 $C_{m 1}$ として認証データ $K_{Pcm 1} / I_{cm 1} / E(K_a, H(K_{Pcm 1} / I_{cm 1}))$ を保持する認証データ保持部 202 と、クラス秘密鍵 $K_{cm 1}$ を保持する K_{cm} 保持部 204 と、個別秘密鍵 $K_{om 2}$ を保持する K_{om} 保持部 206 と、個別秘密鍵 $K_{om 2}$ によって復号可能な個別公開鍵 $K_{Pom 2}$ を保持する K_{Pom} 保持部 208 とを含む。

【0084】

このように、ハードディスクドライブというデータ記憶装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたコンテンツ鍵の管理をハードディスクドライブ単位で実行することが可能になる。

【0085】

HD20は、さらに、端末装置10のHDインターフェース部110と端子210を介して信号を授受するATA (A T t a c h m e n t) インターフェース部212と、HD20におけるデータ伝送路であるバスBS3と、ATAインターフェース部212からコントローラ214を介してバスBS3に出力されたデータを、Kom保持部206により与えられた個別秘密鍵Kom2により復号し、ライセンス提供装置40から配信されたライセンスLICをセキュアデータ記憶部250へ出力する復号処理部216と、KPa保持部218から認証鍵KPaを受け、バスBS3に出力されたデータの認証鍵KPaによる復号処理を実行して復号結果をコントローラ214へ出力し、かつ、得られたクラス公開鍵KPCM1を暗号処理部222へ出力する認証部220と、切換スイッチ260によって選択的に与えられるセッション鍵Ks1xまたはKs2xによって、切換スイッチ262によって選択的に与えられるデータを暗号化してバスBS3に出力する暗号処理部224とを含む。

【0086】

HD20は、さらに、配信、複製・移動、および再生許諾の各セッションにおいて、セッション鍵Ks1x、Ks2xを発生するセッション鍵発生部226と、セッション鍵発生部226の出力したセッション鍵Ks1xを認証部220によって得られる端末装置10の再生回路150のクラス公開鍵KPCpyあるいは他のデータ記憶装置 (HD21とする) のクラス公開鍵KPCM yによって暗号化してバスBS3に送出する暗号処理部222と、バスBS3よりセッション鍵Ks2xによって暗号化されたデータを受けてセッション鍵発生部226より得たセッション鍵Ks1xまたはKs2xによって復号する復号処理部228とを含む。

【0087】

HD20は、さらに、バスBS3上のデータをクラス公開鍵 KP_{cm1} と対をなすクラス秘密鍵 K_{cm1} によって復号するための復号処理部230と、ライセンスLICをHD20からHD21へ移動または複製するために出力する際に、提供先のHD21から受信した個別公開鍵 KP_{omz} ($z \neq 2$) によりライセンスLICを暗号化する暗号処理部232とを含む。

【0088】

HD20は、さらに、暗号化コンテンツデータE (K_c, D_c) を再生するためのライセンスLICと、HD20が処理しているセッションの処理記録であるログとをバスBS3より受けて記憶するセキュアデータ記憶部250を含む。そして、ライセンスLICは、セキュアデータ記憶部250内のセキュアデータメモリ250Aに格納され、ログは、セキュアデータ記憶部250内のログメモリ250Bに格納される。セキュアデータ記憶部250は、たとえば半導体メモリによって構成される。

【0089】

図7は、セキュアデータ記憶部250におけるメモリ構成を示した図である。

図7を参照して、セキュアデータメモリ250Aは、HD20が複数のコンテンツデータを記憶可能であることに対応して、ライセンスLIC (コンテンツ鍵 K_c 、制御情報AC、ライセンスID (LID)、データID (DID)) を複数格納することができる構成になっている。

【0090】

そして、HD20においては、セキュアデータメモリ250Aに格納されたライセンスLICは、セキュアデータ記憶部250における格納アドレス (以下、LBA; Logical Block Addressと称する。) により管理される。そして、各セッションにおいて記憶あるいは出力されるライセンスLICは、全てLBAにより特定される。

【0091】

また、セキュアデータ記憶部250には、有効フラグメモリ250Cが設けられる。有効フラグメモリ250Cは、セキュアデータメモリ250A上の記憶位置を特定するLBAそれぞれに対応して設けられ、対応するLBAによって特定

される位置に記憶されるライセンスの有効性を示すフラグを記憶する。

【0092】

有効フラグメモリ250Cのフラグが「有効」であるとき、フラグに対応するLBAによって特定されるセキュアデータメモリ250A上の記憶位置に記憶されているライセンスLICは利用可能であり、ユーザはそのライセンスLICに対応したコンテンツデータを再生したり、そのライセンスLICの移動・複製を行なうことができる。

【0093】

一方、有効フラグメモリ250Cのフラグが「無効」であるとき、そのフラグに対応するLBAによって特定されるセキュアデータメモリ250A上の記憶位置に記憶されているライセンスLICは利用不可であり、HD20のコントローラ214によって、そのLBAからのライセンスLICは拒否される。すなわち、消去されたのと同じ状態である。したがって、ユーザはそのライセンスLICに対応したコンテンツデータを再生することはできない。この有効フラグメモリ250Cのフラグは、ライセンスの新たな記憶によって「有効」とされ、ライセンスの移動によって「無効」とされる。

【0094】

ログメモリ250Bには、セッションの対象となるライセンスLICを特定するライセンスID(LID)を格納するライセンスID領域2501、セッションにおいてライセンスLICの受信側のデータ記憶装置によって生成されたセッション鍵Ks2xを格納するKs2x領域2502、動作中のセッションにおける処理の状態を示すステータスST1を格納するST1領域2503およびライセンスID領域2501に格納されるライセンスIDに対応したライセンスの記憶状態を示すステータスST2を格納するST2領域2504、ライセンスを移動・複製によって出力する場合、送信側のデータ記憶装置において受信側のデータ記憶装置のクラス公開鍵Kpctxを格納するKpctx領域2505、並びに当該セッションにおいてライセンスLICを出力あるいは記憶するために指示されたLBAを格納するLBA領域2506が設けられ、一連のセッションの処理が進行するにつれて、上記各領域のデータが更新あるいは参照されていく。ス

ステータスST1は、「受信待」、「受信済」、「送信待」および「送信済」の4状態のいずれかであり、ステータスST2は、「データ有」、「データ無」および「移動済」の3状態のいずれかである。

【0095】

そして、セッション中に予期しない異常が発生し、セッションが中断した場合、そのセッションにおいて送受信されていたライセンスLICに対して、ログメモリ250B内のLID領域2501に格納されているライセンスIDと、LBA領域2506に格納されたLBAとによって当該ライセンスLICの記憶状態が確認され、その確認結果に応じてステータスST2が更新される。また、中断したセッションにおけるライセンスの送信側では、ライセンスの受信側のログメモリ250B内に格納されているライセンスLIC、セッション鍵Ks2x、ステータスST1およびステータスST2を受取って、自身が記録するログの内容と受取ったライセンスLIC、セッション鍵Ks2x、ステータスST1およびステータスST2とを確認することにより、再度のライセンスの送受信を行ってもよいか否かの判断がされる。

【0096】

なお、セッション鍵Ks2xは、各セッションを特定するために記憶され、セッション鍵Ks2xを共有していることは、ライセンスの送受信先およびその処理を共有していたことを示している。

【0097】

このような構成とすることにより、特に、相当数のライセンスがセキュアデータメモリ250Aに格納されているときに、あるセッションにおける処理の中断が発生したときなどセキュアデータメモリ250Aにおけるライセンスを特定する必要があるときに（あるいはライセンスの有無を特定）、容易にライセンスの記憶状態を確認し、ステータスST2を更新できる。

【0098】

なお、以下、再送信の確認時においてライセンスの受信側となった場合に、ライセンスの送信側に対して出力するログメモリ250Bに格納されたライセンスID（LID）、セッション鍵Ks2xおよびステータスST1、ST2は、出

カログと総称する。また、HD 2 0 においてのみ参照されるログメモリ 2 5 0 B に格納された受信側のクラス公開鍵 K P c m x および L B A は、内部ログと総称する。

【 0 0 9 9 】

また、ステータス S T 2 には、出力ログが出力される際に、ログメモリ 2 5 0 B に格納されているライセンス I D (L I D) と L B A とによってセキュアデータメモリ 2 5 0 A における対象のライセンスの記憶状態が格納され、これによって出力ログが成立する。

【 0 1 0 0 】

詳細については、後ほど各セッション毎のフローチャートを使用して説明する。

【 0 1 0 1 】

ここで、再び図 6 を参照して、HD 2 0 のデータ記録部に関して説明する。HD 2 0 は、さらに、暗号化コンテンツデータを記憶するノーマルデータ記憶部 2 7 0 を含む。ノーマルデータ記憶部 2 7 0 は、データが記憶される円盤状の磁気記録媒体 2 7 0 1 と、磁気記録媒体 2 7 0 1 を回転させるモータ 2 7 0 2 と、モータ 2 7 0 2 を制御するサーボ制御部 2 7 0 3 と、磁気記録媒体 2 7 0 1 上における磁気ヘッドの位置を制御するシーク制御部 2 7 0 4 と、磁気ヘッドへデータの記録および再生を指示する記録再生処理部 2 7 0 5 とを含む。ノーマルデータ記憶部 2 7 0 の構成は、一般の公知のハードディスクの構成と変わるところはなく、詳細な説明は省略する。

【 0 1 0 2 】

HD 2 0 は、さらに、A T A インターフェース部 2 1 2 を介して外部との間でデータ授受、制御情報 A C に基づくライセンスの出力に関する判断、およびセキュアデータ記憶部 2 5 0 の管理などの HD 2 0 内の動作を制御するためのコントローラ 2 1 4 を含む。

【 0 1 0 3 】

なお、ノーマルデータ記憶部 2 7 0 、A T A インターフェース部 2 1 2 および端子 2 1 0 を除く他の構成は、耐タンパモジュール領域に構成される。

【0104】

以下、図1に示すデータ配信システムにおける各セッションの動作について説明する。

【0105】

〔配信〕

まず、図1に示すデータ配信システムにおいて、ライセンス提供装置40から端末装置10に装着されたHD20へライセンスを配信する動作について説明する。

【0106】

図8および図9は、図1に示すデータ配信システムにおいて、端末装置10のユーザが端末装置10から暗号化コンテンツデータのライセンス配信のリクエストを行なうことにより、ライセンス提供装置40から端末装置10に装着されたHD20へライセンスの配信が行なわれる際の処理（配信セッション）を説明するための第1および第2のフローチャートである。

【0107】

図8における処理開始以前に、端末装置10のユーザは、端末装置10をモデム106によりネットワーク30に接続し、端末装置10をネットワーク30を介してライセンス提供装置40に接続していることを前提としている。

【0108】

図8を参照して、端末装置10のユーザから所望のコンテンツデータのライセンスに対する配信リクエストがなされると、端末装置10のコントローラ108は、バスBS2およびHDインターフェース部110を介してHD20へクラス証明書の出力要求を出力する（ステップS1）。HD20のコントローラ214は、端子210およびATAインターフェース部212を介してクラス証明書の出力要求を受理すると（ステップS2）、バスBS3を介して認証データ保持部202からクラス証明書 $C_{m1} = KP_{cm1} // I_{cm1} // E(K_a, H(KP_{cm1} // I_{cm1}))$ を読み出し、クラス証明書 C_{m1} をATAインターフェース部212および端子210を介して端末装置10へ出力する（ステップS3）。

【0109】

端末装置10のコントローラ108は、HD20からHDインターフェース部110およびバスBS2を介してクラス証明書Cm1を受信すると（ステップS4）、受信したクラス証明書Cm1をモデム106およびネットワーク30を介してライセンス提供装置40へ送信する（ステップS5）。

【0110】

ライセンス提供装置40では、端末装置10からクラス証明書Cm1を受信すると（ステップS6）、受信したCm1が正当なクラス証明書であるか否かを検証する（ステップS7）。検証処理は次のように行なわれる。

【0111】

ライセンス提供装置40は、クラス証明書 $Cm1 = KP_{cm1} // I_{cm1} // E(Ka, H(KP_{cm1} // I_{cm1}))$ を受信すると、HD20から出力されたクラス証明書Cm1に含まれる署名データ $E(Ka, H(KP_{cm1} // I_{cm1}))$ を認証部418において認証鍵KPaで復号する。そして、さらに、認証部418は、クラス証明書Cm1に含まれる $KP_{cm1} // I_{cm1}$ のハッシュ値を演算し、認証鍵KPaで復号した $H(KP_{cm1} // I_{cm1})$ の値と比較する。配信制御部412は、認証部418における復号処理結果から、上記の復号ができ、かつ、ハッシュ値の値が一致したと判断すると、HD20から受信したクラス証明書Cm1は、正当な証明書であると判断する。

【0112】

ステップS7において、クラス証明書Cm1が正当な証明書であると判断された場合、配信制御部418は、クラス証明書Cm1を承認し、クラス公開鍵 KP_{cm1} を受信する（ステップS8）。そして、次の処理（ステップS9）へ移行する。正当なクラス証明書でない場合には、配信制御部412はクラス証明書Cm1を非承認とし、クラス証明書Cm1を受信しないでエラー通知を端末装置10へ出力し（図9のステップS44）、端末装置10においてエラー通知が受理されると（図9のステップS45）、配信セッションが終了する。

【0113】

認証の結果、ライセンス提供装置40において、正当なクラス証明書を持つハ

ードディスクを装着した端末装置からのアクセスであることが確認され、ステップS8においてクラス公開鍵 KP_{cm1} が受理されると、配信制御部412は、ライセンスID(LID)を生成し(ステップS9)、さらに制御情報ACを生成する(ステップS10)。そして、セッション鍵発生部414は、配信のためのセッション鍵 $Ks1a$ を生成する(ステップS11)。セッション鍵 $Ks1a$ は、認証部418によって得られたHD20に対応するクラス公開鍵 KP_{cm1} によって、暗号処理部420によって暗号化され、暗号データE(KP_{cm1} , $Ks1a$)が生成される(ステップS12)。

【0114】

そして、配信制御部412は、ライセンスID(LID)および暗号化されたセッション鍵 $Ks1a$ を1つのデータ列LID//E(KP_{cm1} , $Ks1a$)として、バスBS1および通信装置450を介して外部に出力する(ステップS13)。

【0115】

端末装置10は、ネットワーク30を介してLID//E(KP_{cm1} , $Ks1a$)を受信すると(ステップS14)、受信したLID//E(KP_{cm1} , $Ks1a$)をHD20へ出力する(ステップS15)。そして、HD20のコントローラ214は、端子210およびATAインターフェース部212を介してLID//E(KP_{cm1} , $Ks1a$)を受理する(ステップS16)。コントローラ214は、バスBS3を介して受理したE(KP_{cm1} , $Ks1a$)を復号処理部230へ与え、復号処理部230は、 K_{cm} 保持部204に保持されるHD20に固有なクラス秘密鍵 K_{cm1} によって復号処理することにより、セッション鍵 $Ks1a$ を復号し、セッション鍵 $Ks1a$ を受理する(ステップS17)。

【0116】

HD20のコントローラ214は、ライセンス提供装置40で生成されたセッション鍵 $Ks1a$ の受理を確認すると、ATAインターフェース部212および端子210を介してその旨を端末装置10に通知する。端末装置10のコントローラ108は、HDインターフェース部110およびバスBS2を介して、HD

20においてセッション鍵 $Ks1a$ が受理された旨の通知を受理すると、HD20において配信動作時に生成されるセッション鍵の生成の要求通知をバスBS2およびHDインターフェース部110を介してHD20へ出力する（ステップS18）。HD20のコントローラ214は、端子210およびATAコントローラ212を介してセッション鍵の生成要求通知を受理すると、セッション鍵発生部226に対してHD20において配信動作時に生成されるセッション鍵 $Ks2a$ の生成を指示する。そして、セッション鍵発生部226は、セッション鍵 $Ks2a$ を生成する（ステップS19）。

【0117】

セッション鍵発生部226は、セッション鍵 $Ks2a$ を生成すると、バスBS3を介してコントローラ214へ出力し、セッション鍵 $Ks2a$ を受けたコントローラ214は、ステップS16において受理したライセンスID（LID）とセッション鍵 $Ks2a$ とをセキュアデータ記憶部250内のログメモリ250Bへ格納するとともに、ステータスST1を「受信待」にする（ステップS20）。

【0118】

続いて、暗号処理部224は、切換スイッチ260の接点Pbを介して復号処理部230より与えられるセッション鍵 $Ks1a$ によって、切換スイッチ262の接点PdとPfとを順に切換えることによって与えられるセッション鍵 $Ks2a$ と個別公開鍵 $KPom2$ とからなる1つのデータ列を暗号化し、 $E(Ks1a, Ks2a//KPom2)$ 生成する（ステップS21）。そして、暗号処理部224は、 $E(Ks1a, Ks2a//KPom2)$ をバスBS3に出力する。バスBS3に出力された暗号化データ $E(Ks1a, Ks2a//KPom2)$ は、コントローラ214により受理され、コントローラ214は、受理した暗号化データとライセンスID（LID）とを1つのデータ列としたデータ $LID//E(Ks1a, Ks2a//KPom2)$ をATAインターフェース部212および端子210を介して端末装置10へ出力する（ステップS22）。

【0119】

そして、端末装置10は、データ $LID//E(Ks1a, Ks2a//KP$

om2)をHD20から受理すると(ステップS23)、受理したデータをネットワーク30を介してライセンス提供装置40に出力する(ステップS24)。

【0120】

ライセンス提供装置40は、データLID//E(Ks1a, Ks2a//KPom2)を受信すると(ステップS25)、復号処理部422においてセッション鍵Ks1aによる復号処理を実行し、HD20で生成されたセッション鍵Ks2a、およびHD20の個別公開鍵KPom2を受理する(ステップS26)。

【0121】

配信制御部412は、ライセンスID(LID)に対応するデータID(DID)およびコンテンツ鍵KcをコンテンツDB402から取得し(ステップS27)、ライセンスID(LID)および制御情報ACと併せた1つのデータ列としてのライセンスLIC=Kc//AC//DID//LIDを生成する。

【0122】

配信制御部412は、生成したライセンスLICを暗号処理部424に与える。暗号処理部424は、復号処理部422によって得られたHD20の個別公開鍵KPom2によってライセンスLICを暗号化して暗号化データE(KPom2, LIC)を生成する(ステップS28)。そして、暗号処理部426は、暗号処理部424から受ける暗号化データE(KPom2, LIC)を、復号処理部422から受けるセッション鍵Ks2aによって暗号化し、暗号化データE(Ks2a, E(KPom2, LIC))を生成する(ステップS29)。

【0123】

図9を参照して、配信制御部412は、バスBS1および通信装置450を介して暗号化データE(Ks2a, E(KPom2, LIC))を外部へ出力する(ステップS30)。端末装置10は、ネットワーク30を介して暗号化データE(Ks2a, E(KPom2, LIC))を受理すると(ステップS31)、受理した暗号化データをHD20へ出力する(ステップS32)。

【0124】

HD20のコントローラ214は、端子210およびATAインターフェース

部212を介して暗号化データE (Ks2a, E (KPom2, LIC)) を受理すると(ステップS33)、バスBS3へ出力する。復号処理部228は、セッション鍵発生部226から与えられたセッション鍵Ks2aを用いてバスBS3に出力されたデータE (Ks2a, E (KPom2, LIC)) を復号し、HD20において、ライセンスLICが個別公開鍵KPom2により暗号化された暗号化ライセンスE (KPom2, LIC) が受理される(ステップS34)。そして、復号処理部228は、暗号化ライセンスE (KPom2, LIC) をバスBS3へ出力する。

【0125】

コントローラ214の指示によって、暗号化ライセンスE (KPom2, LIC) は、復号処理部216において個別秘密鍵Kom2によって復号され、ライセンスLICが受理される(ステップS35)。

【0126】

HD20のコントローラ214は、ライセンスLICの受理を確認すると、ATAインターフェース部212および端子210を介してその旨を端末装置10に通知する。端末装置10のコントローラ108は、HDインターフェース部110およびバスBS2を介して、HD20においてライセンスLICが受理された旨の通知を受理すると、HD20のセキュアデータ記憶部250において、その受信したライセンスLICを格納するLBAをバスBS2およびHDインターフェース110を介してHD20へ出力する(ステップS36)。HD20のコントローラ214は、端子210およびATAインターフェース部212を介してライセンスLICの格納先LBAを受理すると(ステップS37)、その受理したLBAをログメモリ250Bに記憶する(ステップS38)。

【0127】

そして、コントローラ214は、受理したライセンスLICに含まれるライセンスID (LID) と、ステップS16において受理したライセンスLID (LID) とを比較し、一致しているか否かをチェックする(ステップS39)。コントローラ214は、LIDが一致しており、受理したライセンスLICが正しいものであると判断すると、端末装置10から受理したセキュアデータ記憶部2

50内のLBAに、受理したライセンスLICを記憶する（ステップS40）。

【0128】

コントローラ214は、指定されたLBAにライセンスLICを記憶すると、有効フラグメモリ250CのそのLBAに対応するフラグを「有効」にする（ステップS41）。そして、コントローラ214は、さらに、ログメモリ250BのステータスST1を「受信済」にし（ステップS42）、配信セッションにおける一連の処理が終了したことを端末装置10に通知する。

【0129】

そして、端末装置10において、HD20から処理終了通知が受理されると、データ配信システムにおける配信セッションが正常終了する。

【0130】

一方、ステップS39において、コントローラ214は、LIDが一致せず、受理したライセンスLICが正しくないと判断すると、エラー通知を端末装置10へ出力し（ステップS43）、端末装置10は、エラー通知を受理すると（ステップS45）、処理を終了する。

【0131】

図8および図9に示された配信処理においては、ライセンス提供装置40における処理履歴の記録に関する記載がなされていないが、図4に示すように、ライセンス提供装置40には、十分な記憶容量を持つログDB404が備えられており、配信セッションにおける各処理の進行に伴う処理履歴がログDB404に記憶される。また、ログDB404には、ライセンスの送信に伴う課金情報なども記憶される。

【0132】

図8および図9に示された配信処理における一連の処理において、ステップS25からステップS44の処理中に異常が発生して処理が中断したときは、再書込処理の対象となる。たとえば、中断の理由として、上記処理中に端末装置10の電源が遮断されたり、ライセンス提供装置40側の異常、あるいは端末装置10とライセンス提供装置40との通信異常など、種々の異常ケースが考えられる。ここで、HD20内のログメモリ250Bに格納されたステータスST2を除

く出力ログの内容がすべて格納されたステップ S 2 2 終了後からステップ S 4 4 までの処理中に処理が中断した場合には、H D 2 0 は、再書込処理を行なってライセンスの提供を受けることが可能である。ここでは、端末装置 1 0 の判断によって再書込処理を行なうものとしたため、端末装置 1 0 において処理の進行が確認できるステップ S 2 2 からステップ S 2 4 を除く、ステップ S 2 5 からステップ S 4 4 の処理中に処理が中断した場合を再書込処理の対象とし、他のステップにおける処理の中断においてはライセンス提供装置 4 0 からライセンスの提供がなされなかったものと判断し、図 8 および図 9 に示したフローチャートにしたがって、最初から処理を行なうこととした。

【 0 1 3 3 】

同様に、ライセンス提供装置 4 0 がライセンスを出力するまでのライセンス提供装置 4 0 内のステップ S 2 5 からステップ S 3 0 までの処理については、端末装置 1 0 において、これらのいずれのステップを処理中に処理が中断したかを特定できる場合には、再書込処理の対象から除外して、図 8 および図 9 に示したフローチャートにしたがって、最初から処理を行なうものとしてもよい。

【 0 1 3 4 】

図 1 0 から図 1 2 は、図 8 および図 9 において示した配信処理におけるステップ S 2 5 からステップ S 4 4 の処理中に異常が発生したときに行なわれる再書込処理の第 1 から第 3 のフローチャートである。

【 0 1 3 5 】

図 1 0 を参照して、端末装置 1 0 は、ステップ S 2 5 からステップ S 4 4 の処理中に異常が発生したと判断すると、ライセンス L I C の再書込要求をネットワーク 3 0 を介してライセンス提供装置 4 0 へ出力する（ステップ S 1 0 1）。配信制御部 4 1 2 は、通信装置 4 5 0 およびバス B S 1 を介して再書込要求を受理すると（ステップ S 1 0 2）、セッション鍵発生部 4 1 4 にセッション鍵を生成するように指示する。指示を受けたセッション鍵発生部 4 1 4 は、再書込処理のためのセッションキー鍵 K s 1 b を生成する（ステップ S 1 0 3）。そして、配信制御部 4 1 2 は、このセッションにおいて H D 2 0 とやり取りしたログが格納されているログ D B 4 0 2 から H D 2 0 に対応するクラス公開鍵 K P c m 1 を取

得し（ステップS104）、暗号処理部420に与える。クラス公開鍵 KP_{cm1} を受けた暗号処理部420は、クラス公開鍵 KP_{cm1} をによりセッション鍵 $Ks1b$ を暗号化し、 $E(KP_{cm1}, Ks1b)$ が生成される（ステップS105）。そして、配信制御部412は、 $E(KP_{cm1}, Ks1b)$ をバスBS1および通信装置450を介して外部に出力する（ステップS106）。

【0136】

端末装置10は、ネットワーク30を介して $E(KP_{cm1}, Ks1b)$ を受理すると（ステップS107）、受理した $E(KP_{cm1}, Ks1b)$ をHD20へ出力する（ステップS108）。そして、HD20のコントローラ214は、端子210およびATAインタフェース部212を介して $E(KP_{cm1}, Ks1b)$ を受理する（ステップS109）。コントローラ214は、受理した $E(KP_{cm1}, Ks1b)$ をバスBS3を介して復号処理部230へ与え、復号処理部230は、 K_{cm} 保持部204に保持されるHD20に固有なクラス秘密鍵 K_{cm1} によって復号処理することにより、セッション鍵 $Ks1b$ を復号し、セッション鍵 $Ks1b$ が受理される（ステップS110）。

【0137】

HD20のコントローラ214は、ライセンス提供装置40で生成されたセッション鍵 $Ks1b$ の受理を確認すると、ATAインターフェース部212および端子210を介してその旨を端末装置10に通知する。端末装置10のコントローラ108は、HDインターフェース部110およびバスBS2を介して、HD20においてセッション鍵 $Ks1b$ が受理された旨の通知を受理すると、セキュアデータ記憶部250に記憶されたログメモリ250Bの出力要求をバスBS2およびHDインターフェース部110を介してHD20へ出力する（ステップS111）。

【0138】

HD20のコントローラ214は、端子210およびATAコントローラ212を介してログメモリ250Bの出力要求通知を受理すると（ステップS112）、ログメモリ250Bに格納されたLBAに記憶されるライセンスLICのライセンスID（LID）と、ログメモリ250Bに格納されたライセンスID（

L I D) とが一致するか否かをチェックする (ステップ S 1 1 3)。

【0139】

コントローラ 2 1 4 は、両ライセンス I D (L I D) が一致すると判断すると、配信処理としては、ライセンス提供装置 4 0 からのライセンス L I C の受理までは行なわれ、H D 2 0 においてライセンス L I C は受理していると認識する。そうすると、コントローラ 2 1 4 は、ログメモリ 2 5 0 B に格納された L B A により指示されるアドレスに記憶されるライセンスに対応する有効フラグメモリ 2 5 0 C に格納されているフラグをチェックして、そのライセンスの有効性をチェックする (ステップ S 1 1 4)。

【0140】

コントローラ 2 1 4 は、ライセンスが有効であると判断すると、ログメモリ 2 5 0 B のステータス S T 2 を「データ有」に変更し、次の処理 (ステップ S 1 1 8) へ移行する。一方、コントローラ 2 1 4 は、ステップ S 1 1 4 においてライセンスが無効であると判断すると、ログメモリ 2 5 0 B のステータス S T 2 を「移動済」に変更し、次の処理 (ステップ S 1 1 8) へ移行する。

【0141】

ステップ 1 1 3 において、コントローラ 2 1 4 は、比較したライセンス I D (L I D) が一致しないと判断したときは、ログメモリ 2 5 0 B のステータス S T 2 を「データ無」に変更する (ステップ S 1 1 7)。

【0142】

このように、ログメモリ 2 5 0 B に格納された L B A を用いて、その L B A に記憶されるライセンス L I C のライセンス I D (L I D) を L B A に基づいて直接確認できるので、セキュアデータメモリ 2 5 0 A に相当数のライセンスが格納されているときであっても、それらのライセンスを逐一検索することなしに特定のライセンス I D (L I D) の有無などを判断することができる。

【0143】

ステータス S T 2 の変更処理がなされると、コントローラ 2 1 4 は、ログメモリ 2 5 0 B からライセンス I D (L I D)、ステータス S T 1、S T 2 およびセッション鍵 K s 2 c を取得する (ステップ S 1 1 8)。ここで、ログメモリ 2 5

0Bに格納されているセッション鍵はKs2aであるが、表記の関係上、ログメモリ250Bから取得したセッション鍵をKs2cとしている。そして、コントローラ214は、取得したセッション鍵Ks2cをバスBS3を介して暗号処理部224へ出力する。

【0144】

暗号処理部224は、切換スイッチ260の接点Pbを介して復号処理部230より与えられるセッション鍵Ks1bによって、バスBS3から取得したセッション鍵Ks2cを暗号化し、 $E(Ks1b, Ks2c)$ 生成する(ステップS119)。そして、暗号処理部224は、生成した $E(Ks1b, Ks2c)$ をバスBS3に出力する。バスBS3に出力された $E(Ks1b, Ks2c)$ は、コントローラ214により受理され、コントローラ214は、ステップS118において取得したデータとともに1つのデータ列 $LID//E(Ks1b, Ks2c)//ST1//ST2$ を生成し、ハッシュ関数を用いてハッシュ値 $H(LID//E(Ks1b, Ks2c)//ST1//ST2)$ を生成する(ステップS120)。そして、コントローラ214は、ハッシュ値 $H(LID//E(Ks1b, Ks2c)//ST1//ST2)$ をバスBS3を介して暗号処理部224へ出力する。

【0145】

暗号処理部224は、切換スイッチ260の接点Pbを介して復号処理部230より与えられるセッション鍵Ks1bによって、バスBS3から取得したハッシュ値 $H(LID//E(Ks1b, Ks2c)//ST1//ST2)$ を暗号化し、 $E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))$ 生成する(ステップS121)。そして、暗号処理部224は、生成した $E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))$ をバスBS3に出力する。ここで、データ列 $LID//E(Ks1b, Ks2c)//ST1//ST2$ を受信ログと称し、 $E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))$ は、受信ログに対してセッション鍵Ks1bを用いて電子署名を行なった署名データである。また、ログメモリ250Bに格納されていたセッション鍵Ks2cをセッション鍵Ks1

bを用いて暗号化するのは、セッション鍵 K_{s2c} の漏洩によるライセンスの流出の危険性を排除するためである。

【0146】

コントローラ214は、バスBS3から署名データを受理すると、ステップS118において取得した受信ログを用いて、署名付き受信ログ $LID//E(K_{s1b}, K_{s2c})//ST1//ST2//E(K_{s1b}, H(LID//E(K_{s1b}, K_{s2c})//ST1//ST2))$ を生成し、ATAインターフェース部212および端子210を介して端末装置10へ出力する(ステップS122)。

【0147】

端末装置10は、署名付き受信ログ $LID//E(K_{s1b}, K_{s2c})//ST1//ST2//E(K_{s1b}, H(LID//E(K_{s1b}, K_{s2c})//ST1//ST2))$ をHD20から受理すると(ステップS123)、受理したデータをネットワーク30を介してライセンス提供装置40へ出力する(ステップS124)。そして、ライセンス提供装置40は、ネットワーク30を介して署名付き受信ログ $LID//E(K_{s1b}, K_{s2c})//ST1//ST2//E(K_{s1b}, H(LID//E(K_{s1b}, K_{s2c})//ST1//ST2))$ を受信する。(ステップS125)

図11を参照して、ライセンス提供装置40は、受信した署名付き受信ログ $LID//E(K_{s1b}, K_{s2c})//ST1//ST2//E(K_{s1b}, H(LID//E(K_{s1b}, K_{s2c})//ST1//ST2))$ の検証を行なう(ステップS126)。検証処理は次のように行なわれる。

【0148】

配信制御部412は、署名付き受信ログを受理すると、まず、受理した署名付き受信ログの後半部である署名データ $E(K_{s1b}, H(LID//E(K_{s1b}, K_{s2c})//ST1//ST2))$ を復号処理部422へ出力するとともに、セッション鍵発生部414にセッション鍵 K_{s1b} を発生するように指示する。そして、復号処理部422は、セッション鍵 K_{s1b} によって署名データ $E(K_{s1b}, H(LID//E(K_{s1b}, K_{s2c})//ST1//ST2))$

）を復号する。一方、配信制御部412は、署名付き受信ログの前半部である受信ログLID//E(Ks1b, Ks2c)//ST1//ST2のハッシュ値を演算し、復号処理部422により復号されたH(LID//E(Ks1b, Ks2c)//ST1//ST2)の値と比較する。配信制御部412は、復号処理部422における復号処理結果から、上記の復号ができ、かつ、ハッシュ値が一致したと判断すると、HD20から受理したデータ列は、正当なデータを含むものとしてライセンス提供装置40において認証される。

【0149】

ステップS126においてHD20から受理した署名付き受信ログが認証されると、配信制御部412は、受理したライセンスID(LID)に基づいてログDB404を検索する(ステップS127)。配信制御部412は、受理したライセンスID(LID)がログDB404内に格納されており、HD20に対して確かに提供を行なったライセンスであると判断すると、受理したステータスST1, ST2の内容を確認する(ステップS128)。

【0150】

配信制御部412は、ステータスST1が「受信待」であり、ステータスST2が「データ無」であるとき、HD20に送信したはずのライセンスLICが何らかの異常によりHD20において受理されていないと判断し、受信したデータ列に含まれる暗号化データE(Ks1b, Ks2c)を復号処理部422へ出力してセッション鍵Ks1bによってセッション鍵Ks2cを復号する。そして、復号されたセッション鍵Ks2cは、バスBS1を介して配信制御部412へ出力され、配信制御部412においてセッション鍵Ks2cが受理される(ステップS129)。

【0151】

そして、配信制御部412は、異常発生時のセッション鍵Ks2aを今回受理したセッション鍵Ks2cと比較チェックする(ステップS130)。配信制御部412は、セッション鍵Ks2aとセッション鍵Ks2cとが一致していると判断すると、ライセンスLICの再書込に対する許可通知を端末装置10へ出力する(ステップS133)。

【0152】

一方、ステップS126においてHD20から受理したデータ列が認証されなかったとき、ステップS127においてHD20から受理したライセンスID（LID）がログDB404内に格納されておらず、HD20に対して提供を行なったライセンスであると判断できないとき、ステップS128において、HD20においてライセンスLICが受理されたものと判断されたとき、またはステップS130において、セッション鍵Ks2aがセッション鍵Ks2cと一致しないと判断されたときは、配信制御部412は、バスBS1および通信装置450を介してエラー通知を出力し（ステップS131）、端末装置10は、ネットワーク30を介してエラー通知を受理すると（ステップS132）、処理が終了する。すなわち、ライセンス提供装置40において、ライセンスの再書込が拒否されて処理が終了する。

【0153】

端末装置10のコントローラ108は、ステップS133においてライセンス提供装置40が出力した許可通知を受理すると（ステップS134）、HD20において配信動作時に生成されるセッション鍵の生成の要求通知をバスBS2およびHDインターフェース部110を介してHD20へ出力する（ステップS135）。

【0154】

HD20は、ライセンス提供装置40からの再書込処理許可通知に基づいて、端末装置10からセッション鍵の生成要求通知を受理すると、以下、図8および図9において説明したステップS19から処理終了までの一連の処理において、セッション鍵Ks2aに代えて新たなセッション鍵Ks2bが生成され、そのセッション鍵Ks2bが使用されるほかは、同様の処理が行なわれる。したがって、ステップS135に続く一連の処理の説明は繰返しになるので省略する。

【0155】

なお、図10～図12のフローチャートに示されるライセンスの配信における再書込処理中の中断に対しては、ステップS101～S131、ステップS133およびステップS142～S160のいずれかのステップにおいて処理が中断

した場合には、再び図10～図12のフローチャートにしたがって再書込処理を行なうことができる。一方、ステップS134～S141のいずれかのステップにおいて処理が中断した場合には、図8および図9のフローチャートに示されるライセンスの配信処理を最初から行なうことによって、処理を再開することができる。

【0156】

このようにして、端末装置10に装着されたHD20が正規のクラス証明書Cm1を保持する機器であることを確認したうえで、クラス証明書Cm1に含まれて送信されたクラス公開鍵KPCm1によってライセンス提供装置40およびHD20でそれぞれ生成される暗号鍵（セッション鍵）をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができる。これによって、不正なハードディスクへのライセンスの配信を禁止することができ、データ配信システムのセキュリティを向上させることができる。

【0157】

さらに、ライセンスの配信処理が中断しても、受信側のデータ記憶装置であるHD20における受信ログをライセンス提供装置40へ送信することで、ライセンスの重複配信を行なうことなく、ライセンスの再送処理を安全に行なうことができる。

【0158】

その上、HD20においてライセンスを記憶するLBAの指示がなされた場合において、そのLBAをログの一部として記録することによって、配信セッション中に異常が発生したとき、ログメモリ250Bに格納されたLBAにしたがって、そのセッションによって記録されるべきライセンスLICのセキュアデータメモリ250Aにおける記憶状態を、相当数のライセンスを記録できるセキュアデータメモリ250A内の検索を行なうことなく、直接的にチェックすることができ、迅速に受信ログが生成される。したがって、配信処理において迅速な再書込処理を行なうことができる。

【0159】

〔複製・移動〕

図13は、ライセンスの複製・移動が行なわれるシステムの構成を概念的に示した概略図である。図13を参照して、端末装置10にデータ記憶装置として2台のハードディスクHD20, HD21が装着可能であり、端末装置10を介してHD20からHD21へライセンスの複製または移動が行なわれる。

【0160】

ここで、HD21は、HD20と異なるデータ記憶装置であるため、HD20とは異なる個別公開鍵 KP_{om5} と個別秘密鍵 K_{om5} とを保持している。この場合、HD21における識別子 z は、HD20の $z=2$ とは異なる $z=5$ となる。また、HD21のクラスは、HD20のクラスと同じ $y=1$ として以下説明する。すなわち、HD20、HD21とも、クラス証明書 $C_{m1}=KP_{cm1}/I_{cm1}/E(K_a, KP_{cm1}/I_{cm1})$ およびクラス秘密鍵 K_{cm1} を保持する。しかしながら、HD21のクラスがHD20のクラスと異なる($y \neq 1$)場合には、クラス証明書およびクラス秘密鍵も、個別公開鍵および個別秘密鍵と同様に、HD20とは異なったものとなる。

【0161】

図14および図15は、図13に示すライセンスの複製・移動が可能なシステムにおいて、端末装置10のユーザが端末装置10から暗号化コンテンツデータのライセンスの複製または移動のリクエストを行なうことにより、端末装置10を介して端末装置10に装着されたHD20からHD21へライセンスの複製または移動が行なわれる際の処理(複製・移動セッション)を説明するための第1および第2のフローチャートである。

【0162】

図14を参照して、端末装置10のユーザから所望のコンテンツデータのライセンスに対する複製または移動の要求が発せられると、端末装置10のコントローラ108は、バスBS2およびHDインターフェース部110を介してHD21へクラス証明書の出力要求を出力する(ステップS201)。HD21のコントローラ214は、端子210およびATAインターフェース部212を介してク

ラス証明書出力要求を受理すると（ステップS202）、認証データ保持部202からクラス証明書 $Cm1 = KPcm1 // Icm1 // E(Ka, H(KPcm1 // Icm1))$ を読み出し、クラス証明書 $Cm1$ をATAインターフェース部212および端子210を介して端末装置10へ出力する（ステップS203）。

【0163】

端末装置10は、HD21からクラス証明書 $Cm1$ を受理すると（ステップS204）、受理したクラス証明書 $Cm1$ をHD20へ送信する（ステップS205）。

【0164】

HD20では、端末装置10からHD21のクラス証明書 $Cm1$ を受理すると（ステップS206）、受理したHD21のクラス証明書 $Cm1$ が正当なクラス証明書であるか否かを検証する（ステップS207）。検証処理は次のように行なわれる。

【0165】

HD20は、HD21のクラス証明書 $Cm1 = KPcm1 // Icm1 // E(Ka, H(KPcm1 // Icm1))$ を受理すると、HD21のクラス証明書 $Cm1$ に含まれる署名データ $E(Ka, H(KPcm1 // Icm1))$ をHD20の認証部220において認証鍵 KPa で復号する。そして、認証部220は、さらに、クラス証明書 $Cm1$ に含まれる $KPcm1 // Icm1$ のハッシュ値を演算し、認証部220において復号された $H(KPcm1 // Icm1)$ の値と比較する。HD20のコントローラ214は、認証部220における復号処理結果から、上記の復号ができ、かつ、ハッシュ値の値が一致したと判断すると、HD21から受理したクラス証明書 $Cm1$ は、正当な証明書であると判断する。

【0166】

ステップS207において、HD21のクラス証明書 $Cm1$ が正当な証明書であると判断されると、HD20のコントローラ214は、HD21のクラス証明書 $Cm1$ を承認してHD21のクラス証明書 $Cm1$ に含まれるHD21のクラス

公開鍵 KP_{cm1} を受理し、受理した HD_{21} のクラス公開鍵 KP_{cm1} を HD_{20} のセキュアデータ記憶部 250 内のログメモリ $250B$ に格納する（ステップ S_{208} ）。そして、次の処理（ステップ S_{209} ）へ移行する。コントローラ 214 は、正当な HD_{21} のクラス証明書でない場合には、 HD_{21} のクラス証明書 C_{m1} を非承認として受理せず、エラー通知を端末装置 10 へ出力する（図 15 のステップ S_{252} ）。そして、端末装置 10 においてエラー通知が受理されると（図 15 のステップ S_{253} ）、配信セッションが終了する。

【0167】

ステップ S_{207} における検証の結果、 HD_{20} において、 HD_{21} が正当なクラス証明書を持つハードディスクであることが確認され、ステップ S_{208} において HD_{21} のクラス公開鍵 KP_{cm1} が受理されると、 HD_{20} のセッション鍵発生部 226 は、セッション鍵 K_{s1a} を生成する（ステップ S_{209} ）。セッション鍵 K_{s1a} は、認証部 220 によって得られた HD_{21} のクラス公開鍵 KP_{cm1} によって、暗号処理部 222 において暗号化され、暗号化データ $E(KP_{cm1}, K_{s1a})$ が生成される（ステップ S_{210} ）。

【0168】

そして、コントローラ 214 は、ライセンス ID (LID) および暗号化されたセッション鍵 K_{s1a} を1つのデータ列 $LID//E(KP_{cm1}, K_{s1a})$ として、 ATA インターフェース部 212 および端子 210 を介して端末装置 10 へ出力する（ステップ S_{211} ）。

【0169】

ここで、ライセンス ID (LID) は、事前に管理ファイルを参照することで HD_{20} のコントローラ 214 が取得している。管理ファイルは、 HD_{20} に記憶されている暗号化コンテンツデータとライセンスとの関係を管理するための管理データを記録したデータファイルであって、ノーマルデータ記憶部 270 に記憶され、暗号化コンテンツデータの記録消去や、ライセンスの書込、移動および消去によってその内容が更新される。

【0170】

端末装置 10 は、 $LID//E(KP_{cm1}, K_{s1a})$ を受理すると（ステ

ップS212)、受理したLID//E(KPcm1, Ks1a)をHD21へ出力する(ステップS213)。そして、HD21のコントローラ214は、端子210およびATAインタフェース部212を介してLID//E(KPcm1, Ks1a)を受理する(ステップS214)。続いて、コントローラ214は、バスBS3を介してE(KPcm1, Ks1a)を復号処理部230へ与え、復号処理部230は、Kcm保持部204に保持されるHD21に固有なクラス秘密鍵Kcm1によって復号処理することにより、セッション鍵Ks1aを復号し、セッション鍵Ks1aを受理する(ステップS215)。

【0171】

HD21のコントローラ214は、HD20で生成されたセッション鍵Ks1aの受理を確認すると、ATAインターフェース部212および端子210を介してその旨を端末装置10に通知する。端末装置10は、HD21においてセッション鍵Ks1aが受理された旨の通知を受理すると、HD21において複製・移動動作時に生成されるセッション鍵の生成の要求通知をHD21へ出力する(ステップS216)。HD21のコントローラ214は、端子210およびATAコントローラ212を介してセッション鍵の生成要求通知を受理すると、セッション鍵発生部226に対してライセンスの複製・移動時に生成されるセッション鍵の生成を指示する。そして、セッション鍵発生部226は、セッション鍵Ks2aを生成する(ステップS217)。

【0172】

セッション鍵発生部226は、セッション鍵Ks2aを生成すると、バスBS3を介してコントローラ214へ出力し、セッション鍵Ks2aを受けたコントローラ214は、ステップS214において受理したライセンスID(LID)とセッション鍵Ks2aとをHD21のセキュアデータ記憶部250内のログメモリ250Bへ格納し、ステータスST1を「受信待」にする(ステップS218)。

【0173】

続いて、HD21の暗号処理部224は、切換スイッチ260の接点Pbを介して復号処理部230より与えられるセッション鍵Ks1aによって、切換スイ

ッチ262の接点PdとPfとを順に切換えることによって与えられるセッション鍵Ks2aと個別公開鍵KPom5とからなる1つのデータ列を暗号化し、E(Ks1a, Ks2a//KPom5)を生成する(ステップS219)。そして、暗号処理部224は、E(Ks1a, Ks2a//KPom5)をバスBS3に出力する。バスBS3に出力された暗号化データE(Ks1a, Ks2a//KPom5)は、コントローラ214により受理され、コントローラ214は、受理した暗号化データとライセンスID(LID)とを1つのデータ列としたデータLID//E(Ks1a, Ks2a//KPom5)をATAインターフェース部212および端子210を介して端末装置10へ出力する(ステップS220)。

【0174】

そして、端末装置10は、データLID//E(Ks1a, Ks2a//KPom5)をHD21から受理すると(ステップS221)、受理したデータをHD20へ出力する(ステップS222)。

【0175】

HD20は、データLID//E(Ks1a, Ks2a//KPom5)を受理すると(ステップS223)、復号処理部228においてセッション鍵Ks1aによる復号処理を実行し、HD21で生成されたセッション鍵Ks2a、およびHD21の個別公開鍵KPom5を受理する(ステップS224)。そして、復号処理部228は、復号したセッション鍵Ks2aをバスBS3を介してコントローラ214へ出力し、コントローラ214は、ステップS223において受理したライセンスID(LID)とセッション鍵Ks2aとをHD20のセキュアデータ記憶部250内のログメモリ250Bへ格納し、ステータスST1を「送信待」にする(ステップS225)。

【0176】

ステップS225の処理を終えると、HD20のコントローラ214は、その旨をATAインターフェース部212および端子210を介して端末装置10に通知する。端末装置10のコントローラ108は、HDインターフェース部110およびバスBS2を介して、HD20からの通知を受理すると、HD20のセ

セキュアデータ記憶部 2 5 0 において、HD 2 0 から HD 2 1 へ送信するライセンス L I C が格納されている L B A をバス B S 2 および HD インターフェース 1 1 0 を介して HD 2 0 へ出力する（ステップ S 2 2 6）。HD 2 0 のコントローラ 2 1 4 は、端子 2 1 0 および A T A インターフェース部 2 1 2 を介して送信対象のライセンス L I C の格納先 L B A を受理すると（ステップ S 2 2 7）、その受理した L B A をセキュアデータ記憶部 2 5 0 のログメモリ 2 5 0 B に記憶する（ステップ S 2 2 8）。

【0 1 7 7】

そして、コントローラ 2 1 4 は、受理した L B A に格納されるライセンス L I C に対応する有効フラグメモリ 2 5 0 C のフラグが「有効」であるか「無効」であるかを確認する（ステップ S 2 2 9）。コントローラ 2 1 4 は、有効フラグが「有効」であると、受理した L B A に基づいて、その L B A に格納されるライセンス L I C を取得する（ステップ S 2 3 0）。

【0 1 7 8】

図 1 5 を参照して、コントローラ 2 1 4 は、対象のライセンス L I C を取得すると、ライセンス L I C に含まれるライセンス I D (L I D) と、ステップ S 2 2 3 において受理したライセンス I D (L I D) とを比較し、一致しているか否かをチェックする（ステップ S 2 3 1）。コントローラ 2 1 4 は、一致していると判断すると、取得したライセンス L I C に含まれる制御情報 A C を確認して利用制限がかけられていないかをチェックする（ステップ S 2 3 2）。

【0 1 7 9】

コントローラ 2 1 4 は、制御情報 A C においてライセンス L I C の利用が禁止されていないことを確認すると、取得したライセンス L I C を暗号処理部 2 3 2 に与える。暗号処理部 2 3 2 は、復号処理部 2 2 8 によって得られた HD 2 1 の個別公開鍵 K P o m 5 によってライセンス L I C を暗号化して暗号化データ E (K P o m 5, L I C) を生成する（ステップ S 2 3 3）。そして、暗号処理部 2 3 2 は、暗号化データ E (K P o m 5, L I C) を切替スイッチ P c を介して暗号処理部 2 2 4 へ出力し、暗号処理部 2 2 4 は、暗号処理部 2 3 2 から受けた暗号化データを復号処理部 2 2 8 から受けたセッション鍵 K s 2 a によって暗号化

し、暗号化データE (K s 2 a, E (K P o m 5, L I C)) を生成する (ステップS 2 3 4)。

【0180】

続いて、コントローラ214は、対象のライセンスL I Cに含まれる制御情報A Cに基づいて、HD 2 0からHD 2 1へのライセンスL I Cの送信が「移動」であるか「複製」であるかを確認する (ステップS 2 3 5)。コントローラ214は、「移動」であると確認したときは、その対象のライセンスL I Cに対応する有効フラグメモリ250Cのフラグを「無効」に変更する (ステップS 2 3 6)。一方、コントローラ214は、「複製」であると確認したときには、当該ライセンスL I CがHD 2 0に残っていてもよいので、有効フラグメモリ250Cのフラグの変更は行なわずに次の処理 (ステップS 2 3 7) へ移行する。

【0181】

コントローラ214は、有効フラグメモリ250Cの処理が終わると、ログメモリ250BのステータスS T 1を「送信済」に変更し (ステップS 2 3 7)、A T Aインタフェース部212および端子210を介して暗号化データE (K s 2 a, E (K P o m 5, L I C)) を端末装置10へ送信する (ステップS 2 3 8)。

【0182】

一方、ステップS 2 2 9において受理したL B Aに対応する有効フラグメモリ250Cのフラグが「無効」であったとき、ステップS 2 3 1においてライセンスI D (L I D) が一致しないとき、または、ステップS 2 3 2において、取得したライセンスL I Cに含まれる制御情報A Cにより当該ライセンスL I Cの利用が禁止されているときは、コントローラ214は、端末装置10に対してエラー通知を出力し (ステップS 2 5 2)、端末装置10においてエラー通知が受理されると (ステップS 2 5 3)、処理が終了する。

【0183】

端末装置10は、ステップS 2 3 8においてHD 2 0から出力された暗号化データE (K s 2 a, E (K P o m 5, L I C)) を受理すると (ステップS 2 3 9)、受理した暗号化データをHD 2 1へ出力する (ステップS 2 4 0)。HD

21のコントローラ214は、端子210およびATAインターフェース部212を介して暗号化データE(Ks2a, E(KPom5, LIC))を受理すると(ステップS241)、バスBS3へ出力する。復号処理部228は、セッション鍵発生部226から与えられたセッション鍵Ks2aを用いてバスBS3に出力されたデータE(Ks2a, E(KPom5, LIC))を復号し、HD21において、ライセンスLICが個別公開鍵KPom5により暗号化された暗号化ライセンスE(KPom5, LIC)が受理される(ステップS242)。そして、復号処理部228は、暗号化ライセンスE(KPom5, LIC)をバスBS3へ出力する。

【0184】

コントローラ214の指示によって、暗号化ライセンスE(KPom5, LIC)は、復号処理部216において個別秘密鍵Kom5によって復号され、HD21においてライセンスLICが受理される(ステップS243)。

【0185】

コントローラ214は、ライセンスLICの受理を確認すると、ATAインターフェース部212および端子210を介してその旨を端末装置10に通知する。端末装置10のコントローラ108は、HDインターフェース部110およびバスBS2を介して、HD21においてライセンスLICが受理された旨の通知を受理すると、HD21のセキュアデータ記憶部250において、その受信したライセンスLICを格納するLBAをバスBS2およびHDインターフェース110を介してHD21へ出力する(ステップS244)。HD21のコントローラ214は、端子210およびATAインターフェース部212を介してライセンスLICの格納先のLBAを受理すると(ステップS245)、その受理したLBAをログメモリ250Bに記憶する(ステップS246)。

【0186】

そして、コントローラ214は、受理したライセンスLICに含まれるライセンスID(LID)と、ステップS214において受理したライセンスLID(LID)とを比較し、一致しているか否かをチェックする(ステップS247)。コントローラ214は、LIDが一致しており、受理したライセンスLICが

正しいものであると判断すると、端末装置 1 0 から受理したセキュアデータ記憶部 2 5 0 内の L B A に、受理したライセンス L I C を記憶する（ステップ S 2 4 8）。

【 0 1 8 7 】

コントローラ 2 1 4 は、指定された L B A にライセンス L I C を記憶すると、有効フラグメモリ 2 5 0 C のその L B A に対応するフラグを「有効」にする（ステップ S 2 4 9）。そして、コントローラ 2 1 4 は、さらに、ログメモリ 2 5 0 B のステータス S T 1 を「受信済」にし（ステップ S 2 5 0）、複製・移動セッションにおける一連の処理が終了したことを A T A インターフェース部 2 1 2 および端子 2 1 0 を介して端末装置 1 0 に通知する。

【 0 1 8 8 】

そして、端末装置 1 0 において、H D 2 1 からの処理終了通知が受理されると、H D 2 0 および H D 2 1 間の複製・移動セッションが正常終了する。

【 0 1 8 9 】

一方、ステップ S 2 4 7 において、コントローラ 2 1 4 は、L I D が一致しておらず、受理したライセンス L I C が正しくないと判断すると、A T A インターフェース部 2 1 2 および端子 2 1 0 を介してエラー通知を端末装置 1 0 へ出力し（ステップ S 2 5 1）、端末装置 1 0 においてエラー通知が受理されると（ステップ S 2 5 3）、複製・移動セッションが終了する。

【 0 1 9 0 】

ここで、配信セッションのときと同様に、図 1 4 および図 1 5 に示された複製・移動セッションにおける一連の処理において、ステップ S 2 2 7 からステップ S 2 5 2 の処理中に異常が発生し、処理が中断したときは、再書込処理の対象となる。

【 0 1 9 1 】

ここで、図 1 4 および図 1 5 に示された複製・移動セッションにおいて、ステップ S 2 2 7 からステップ S 2 3 5 までの処理を再書込処理の対象としたのは、この一連の処理が H D 2 0 の内部処理であり、ステップ S 2 2 6 の終了後は、ステップ S 2 3 8 まで端末装置 1 0 においていずれのステップを処理中に処理が中

断したかを特定できないため、すべてステップ S 2 3 6 が実行されてライセンスが無効化されたものとし、必ず再書込処理の対象としたものである。

【0192】

そして、ステップ S 2 3 6 からステップ S 2 4 7 までの処理を再書込処理の対象としたのは、移動処理の場合、この間は、HD 2 0 内のライセンスがステップ S 2 3 6 において無効化され、かつ、HD 2 1 内に有効なライセンスが格納されていない状態であって、この間に処理が中断すると、対象となるライセンスが消失してしまうからである。なお、複製処理の場合は、ステップ S 2 3 6 においてライセンスは無効化されないため、移動の場合と同様に再書込処理を行なうようにしても、また、複製処理を最初から行なうようにしてもよい。しかしながら、移動処理の場合は、再書込処理によってのみしかライセンスを復活させることはできない。

【0193】

また、ステップ S 2 4 8 からステップ S 2 5 0 までの処理を再書込処理の対象としたのは、ステップ S 2 4 9, S 2 5 0 については、これらの処理はステップ S 2 4 8 におけるライセンス書込後の処理であるから本来は処理が終了しているところ、端末装置 1 0 からはステップ S 2 4 8 の終了が特定できないため、ステップ S 2 4 8 が終了していないものとみなして、ステップ S 2 4 8 からステップ S 2 5 0 を再書込処理の対象としたものである。なお、ステップ S 2 4 8 が終了していて再書込処理が行なわれた場合には、再書込処理において再書込は拒否される。

【0194】

また、ステップ S 2 5 1 の処理を再書込処理の対象としたのは、本来この処理で処理が中断するのはかなり特殊な場合に限られるものであるが、端末装置 1 0 においては、ステップ S 2 5 1 において処理が中断したことを特定することができないため、再書込処理の対象としたものである。

【0195】

なお、端末装置 1 0 において、上述したように当該セッションがライセンスの複製であると判断できる場合、あるいはステップ S 2 2 7 からステップ S 2 3 5

およびステップS249からステップS251のいずれかのステップで処理が中断したかを特定できる場合においては、必ずしも再書込処理とする必要はなく、図14および図15に示された複製・移動セッションを再度実行すればよい。

【0196】

図16から図18は、図14および図15において示した複製・移動セッションの処理フローにおけるステップS227からステップS252の処理中に異常が発生したときに行なわれる再書込処理の第1から第3のフローチャートである。

【0197】

図16を参照して、端末装置10は、ステップS227からステップS252の処理中に異常が発生したと判断すると、ライセンスLICの再送要求をHD20へ出力する（ステップS301）。HD20のコントローラ214は、端子210およびATAインターフェース部212を介して再送要求を受理すると、セキュアデータ記憶部250内のログメモリ250Bに格納されているステータスST1の状態を確認する（ステップS302）。コントローラ214は、ステータスST1が「送信待」または「送信済」でないとき、すなわち複製・移動セッションにおいてライセンスLICの送信側でないときは、図18に示すステップS371へ処理が移行する。

【0198】

HD20のコントローラ214は、ステータスST1が「送信待」または「送信済」であるときは、セッション鍵発生部226にセッション鍵を生成するように指示し、セッション鍵発生部226は、セッション鍵Ks1aを生成する（ステップS303）。セッション鍵Ks1bが生成されると、コントローラ214は、中断以前に受理してログメモリ250Bに格納されたHD21のクラス公開鍵KPcm1を取得する（ステップS304）。そして、そのHD21のクラス公開鍵KPcm1によって、セッション鍵Ks1bが暗号処理部222によって暗号化され、暗号化データE（KPcm1, Ks1b）が生成される（ステップS305）。コントローラ214は、生成された暗号化データE（KPcm1, Ks1b）をATAインターフェース部212および端子210を介して端末装

置10へ出力する（ステップS306）。

【0199】

端末装置10は、暗号化データE（KPcm1，Ks1b）を受理すると（ステップS307）、受理した暗号化データE（KPcm1，Ks1a）をHD21へ出力する（ステップS308）。HD21のコントローラ214は、端子210およびATAインターフェース部212を介してE（KPcm1，Ks1a）を受理すると（ステップS309）、バスBS3を介してE（KPcm1，Ks1a）を復号処理部230へ与える。そうすると、復号処理部230は、Kcm保持部204に保持されるHD21に固有なクラス秘密鍵Kcm1によって復号処理を実行してセッション鍵Ks1bを復号し、セッション鍵Ks1bを受理する（ステップS310）。

【0200】

HD21のコントローラ214は、HD20で生成されたセッション鍵Ks1bの受理を確認すると、ATAインターフェース部212および端子210を介してその旨を端末装置10に通知する。端末装置10のコントローラ108は、HDインターフェース部110およびバスBS2を介してHD21からの通知を受理すると、HD21のログメモリ250Bに格納されるログのHD20への出力要求をバスBS2およびHDインターフェース部110を介してHD21へ出力する（ステップS311）。HD21のコントローラ214は、端子210およびATAコントローラ212を介してログの出力要求通知を受理すると（ステップS312）、ログメモリ250Bに格納されたLBAに記憶されるライセンスLICのライセンスID（LID）と、ログメモリ250Bに格納されたライセンスID（LID）とが一致するか否かを確認する（ステップS313）。

【0201】

コントローラ214は、ライセンスID（LID）が一致すると、さらに、ログメモリ250Bに格納されたLBAに記憶されるライセンスLICに対応する有効フラグメモリ250Cのフラグを確認し、そのライセンスLICが有効であるか無効であるかを確認する（ステップS314）。コントローラ214は、有効フラグメモリ250Cのフラグが「有効」であるときは、ログメモリ250B

のステータスST2を「データ有」に変更し（ステップS315）、次の処理（ステップS318）へ移行する。一方、コントローラ214は、有効フラグメモリ250Cのフラグが「無効」であるときは、ログメモリ250BのステータスST2を「移動済」に変更し（ステップS316）、次の処理（ステップS318）へ移行する。

【0202】

また、コントローラ214は、ステップS313において両ライセンスID（LID）が一致しないときは、ログメモリ250BのステータスST2を「データ無」に変更する（ステップS317）。

【0203】

このように、複製・移動セッションにおいても、ログメモリ250Bに格納されたLBAを用いて、そのLBAにより指定されるセキュアデータメモリ250Aの記憶位置に記憶されるライセンスのライセンスID（LID）をLBAに基づいて直接確認できるので、セキュアデータメモリ250Aに相当数のライセンスが格納されているときであっても、それらのライセンスを逐一検索することなしにライセンスID（LID）の特定または有無を判断することができる。

【0204】

ステータスST2の変更処理がなされると、コントローラ214は、ログメモリ250BからライセンスID（LID）、ステータスST1、ST2およびセッション鍵Ks2cを取得する（ステップS318）。ここで、ログメモリ250Bに格納されているセッション鍵はKs2aであるが、表記の関係上、ログメモリ250Bから取得したセッション鍵をKs2cとしている。そして、コントローラ214は、取得したセッション鍵Ks2cをバスBS3を介して暗号処理部224へ出力する。

【0205】

暗号処理部224は、切換スイッチ260の接点Pbを介して復号処理部230より与えられるセッション鍵Ks1bによってセッション鍵Ks2cを暗号化し、E（Ks1b, Ks2c）生成する（ステップS319）。そして、暗号処理部224は、生成したE（Ks1b, Ks2c）をバスBS3に出力する。パ

スBS3に出力されたE(Ks1b, Ks2c)は、コントローラ214により受理され、コントローラ214は、ステップS318において取得したデータとともに1つの受信ログLID//E(Ks1b, Ks2c)//ST1//ST2を生成し、そのハッシュ値H(LID//E(Ks1b, Ks2c)//ST1//ST2)を生成する(ステップS320)。そして、コントローラ214は、ハッシュ値H(LID//E(Ks1b, Ks2c)//ST1//ST2)をバスBS3を介して暗号処理部224へ出力する。

【0206】

暗号処理部224は、切換スイッチ260の接点Pbを介して復号処理部230より与えられるセッション鍵Ks1bによって、バスBS3から取得したハッシュ値H(LID//E(Ks1b, Ks2c)//ST1//ST2)を暗号化し、署名データE(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))生成する(ステップS321)。そして、暗号処理部224は、生成したE(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))をバスBS3に出力する。

【0207】

コントローラ214は、バスBS3から署名データを取得すると、ステップS318において取得した受信ログを用いて、署名付き受信ログLID//E(Ks1b, Ks2c)//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))を生成し、ATAインターフェース部212および端子210を介して端末装置10へ出力する(ステップS322)。

【0208】

端末装置10は、署名付き受信ログLID//E(Ks1b, Ks2c)//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))をHD21から受理すると(ステップS323)、受理したデータをHD20へ出力する(ステップS324)。

【0209】

HD20は、署名付き受信ログLID//E(Ks1b, Ks2c)//ST

1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))を受理すると(ステップS325)、受理したデータの検証を行なう(ステップS326)。検証処理は、以下のように行われる。

【0210】

HD20のコントローラ214は、署名付き受信ログを受理すると、まず、受理した署名付き受信ログの後半部である署名データE(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))を復号処理部228へ出力するとともに、セッション鍵発生部226にセッション鍵Ks1bを発生するように指示する。そして、復号処理部228は、セッション鍵Ks1bによって署名データE(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))を復号する。一方、HD20のコントローラ214は、署名付き受信ログの前半部である受信ログLID//E(Ks1b, Ks2c)//ST1//ST2のハッシュ値を演算し、復号処理部228により復号されたH(LID//E(Ks1b, Ks2c)//ST1//ST2)の値と比較する。HD20のコントローラ214は、復号処理部228における復号処理結果から、上記の復号ができ、かつ、ハッシュ値が一致したと判断すると、HD21から受理したデータ列は、正当なデータを含むものとしてHD20において認証される。

【0211】

ステップS326において署名付き受信ログの検証が行なわれ、そのデータがHD20において承認されると、HD20のコントローラ214は、ステップS325において受理したデータに含まれるライセンスID(LID)をログメモリ250Bに格納されるライセンスID(LID)と比較する(ステップS327)。

【0212】

コントローラ214は、ライセンスID(LID)が一致すると、受信したデータ列に含まれる暗号データE(Ks1b, Ks2c)を復号処理部228へ出力し、復号処理部228は、セッション鍵発生部226から受けるセッション鍵Ks1bによってセッション鍵Ks2cを復号し、セッション鍵Ks2cが受理

される（ステップS328）。そして、復号されたセッション鍵K s 2 cは、バスBS3を介してコントローラ214へ出力される。続いて、コントローラ214は、エラー発生時のセッション鍵K s 2 aを今回受理したセッション鍵K s 2 cと比較チェックする（ステップS329）。コントローラ214は、セッション鍵K s 2 aとセッション鍵K s 2 cとが一致していると判断すると、受理したステータスST1、ST2の内容を確認する（ステップS330）。

【0213】

HD20のコントローラ214は、受信したステータスST1が「受信待」であり、ステータスST2が「データ無」であるとき、HD21に送信したはずのライセンスLICが何らかの異常によりHD21において受理されていないと判断する。そうすると、HD20のコントローラ214は、さらに、ログメモリ250Bに格納されたLBAに記憶されるライセンスLICのライセンスID（LID）と、ログメモリ250Bに格納されたライセンスID（LID）とが一致するか否かを確認する（ステップS331）。HD20のコントローラ214は、ライセンスID（LID）が一致すると、さらに、ログメモリ250Bに格納されたLBAに対応する有効フラグメモリ250Cのフラグを確認し、そのライセンスLICが有効であるか無効であるかを確認する（ステップS332）。そして、コントローラ214は、有効フラグメモリ250Cのフラグが「無効」であるときは、その有効フラグメモリ250Cのフラグを「有効」に変更する（ステップS333）。一方、コントローラ214は、有効フラグメモリ250Cのフラグが「有効」であるときは、次の処理（ステップS334）へ移行する。そして、コントローラ214は、ログメモリ250Bに格納されるLBAを取得し、ATAインターフェース部212および端子210を介して端末装置10へ出力する（ステップS334）。

【0214】

端末装置10のコントローラ108は、HD20からHDインターフェース部110およびバスBS2を介して対象のライセンスLICが格納されるLBAを受理すると（ステップS335）、HD21において複製・移動動作時に生成されるセッション鍵の生成の要求通知をバスBS2およびHDインターフェース部

110を介してHD21へ出力する（ステップS336）。

【0215】

HD21は、端末装置10からセッション鍵の生成要求通知を受理すると、以下、図14および図15において説明したステップS217から処理終了までの一連の処理において、セッション鍵Ks2aに代えて新たなセッション鍵Ks2bが生成され、そのセッション鍵Ks2bが使用されるほかは、同様の処理が行なわれる。したがって、ステップS336に続く一連の処理の説明は繰返しになるので省略する。

【0216】

なお、ステップS335において処理を終了し、HD20にライセンスを残すことも可能である。この場合、図14および図15に示したフローチャートにしたがって、再度ライセンスを移動させることができる。

【0217】

なお、図16～図18のフローチャートに示されるライセンスの移動または複製における再書込処理の中断に対しては、ステップS301～S344およびステップS347～S371のいずれかのステップにおいて処理が中断した場合には、再び図16～図18に示されるフローチャートにしたがって再書込処理を行なうことができる。一方、ステップS325～S346のいずれかのステップにおいて処理が中断した場合には、図14および図15のフローチャートに示されるライセンスの移動または複製の処理を最初から行なうことによって、処理を再開することができる。

【0218】

このようにして、端末装置10に装着された複数のハードディスク間におけるライセンスの複製または移動に関しても、複製先または移動先のHD21から受取ったクラス証明書Cm1が有効であることを確認し、クラス証明書Cm1に含まれて送信されたクラス公開鍵KPCm1によってライセンスの複製・移動が行なわれる複数のハードディスク間でそれぞれ生成される暗号鍵（セッション鍵）をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、不正なハードディスクへのライセンス

の複製または移動を禁止することができる。さらには、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、出力先のなりすましからライセンスを保護して、システムのセキュリティを向上させることができる。

【0219】

さらに、ライセンスの複製・移動セッションの中断においても、配信セッションと同様に、受信側のデータ記憶装置であるHD21における複製・移動セッションの対象となったライセンスLICに対する受信ログを送信側のデータ記憶装置であるHD20へ送信し、HD20において、自身のログメモリ250Bに記憶される内容と、ログメモリ250Bに記憶されるLBAによって特定されるセキュアデータメモリ250Aに記憶されるライセンスLICとを比較し、さらに有効フラグメモリ250Cに記憶されるフラグを参照することによって、中断した複製・移動セッションがライセンスの移動を行なう処理である場合において、2つのデータ記憶装置HD20およびHD21に利用可能なライセンスが重複して存在することのない安全な再書込処理が提供される。

【0220】

その上、受信側のデータ記憶装置であるHD21においてライセンスを記憶するLBAの指示がなされた場合において、そのLBAをログの一部として記録することによって、複製・移動セッション中に異常が発生したとき、ログメモリ250Bに格納されたLBAにしたがって、そのセッションによって記録されるべきライセンスLICのセキュアデータメモリ250Aにおける記憶状態を、相当数のライセンスを記録できるセキュアデータメモリ250A内の検索を行なうことなく、直接的にチェックすることができ、迅速に受信ログが生成される。したがって、複製・移動処理においても迅速な再書込処理を行なうことができる。また、送信側のデータ記憶装置であるHD20においても、ダイレクトに処置の対象であるライセンスLICの内容および状態（利用可否）が判断できる。

【0221】

このように、本発明は、複製・移動セッションの中断によるライセンスLICの消失を回避し、迅速な処理を行なうことができるデータ記憶装置およびその処

理手順を提供するとともに、再書込処理に至った場合でも安全に処理が行なわれ、確実な著作権保護を実現することができるデータ記憶装置およびその処理手順を提供する。

【0222】

なお、図14～図18におけるHD21の処理ステップS202, 203, S214, S215, S217～S220, S241～S243, S245～S251, S309, S310, S312～S322, S337～S340, S361～S363, S365～S371は、図8～図12におけるHD20の処理ステップS2, S3, S16, S17, S19～S22, S33～S35, S37～S43, S109, S110, S112～S122, S136～S139, S150～S152, S154～S160とそれぞれ同じである。すなわち、ライセンスの移動または複製時におけるHD21の処理とライセンスの配信処理時におけるHD20の処理とは同じ処理であって、これらの処理は、いずれも、データ記憶装置（HD20, HD21）においてライセンスを書込むためのデータ記憶装置における処理である。

【0223】

〔再生許諾〕

再び図5を参照して、コンテンツデータを再生する再生回路150を備えた端末装置10にデータ記憶装置としてのHD20が装着され、コンテンツデータの再生許諾は、HD20から端末装置10内の再生回路150に対して行なわれる。

【0224】

図19は、端末装置10のユーザが端末装置10から暗号化コンテンツデータの再生リクエストを行なうことにより、端末装置10に装着されたHD20から端末装置10内の再生回路150へ再生許諾が行なわれる際の処理（再生許諾セッション）を説明するためのフローチャートである。

【0225】

図19を参照して、端末装置10のユーザから所望のコンテンツデータの再生リクエストがなされると、端末装置10のコントローラ108は、バスBS2を

介して再生回路150へクラス証明書C_p3の出力要求を出力する（ステップS401）。再生回路150において、認証データ保持部1502は、バスBS2からクラス証明書C_p3の出力要求を受けると（ステップS402）、保持しているクラス証明書C_p3=K_{Pcp}3//I_{cp}3//E（K_a, H（K_{Pcp}3//I_{cp}3））をバスBS2へ出力する（ステップS403）。

【0226】

コントローラ108は、バスBS2からクラス証明書C_p3を受理すると（ステップS404）、受理したクラス証明書C_p3をバスBS2およびHDインターフェース部110を介してHD20へ出力する（ステップS405）。

【0227】

HD20では、端末装置10からクラス証明書C_p3を受理すると（ステップS406）、受理したクラス証明書C_p3が正当なクラス証明書であるか否かを検証する（ステップS407）。検証処理は、複製・移動セッションにおけるステップS207において説明したのと同様の方法で行なわれ、説明は省略する。

【0228】

ステップS407において、クラス証明書C_p3が正当な証明書であると判断された場合、コントローラ214は、クラス証明書C_p3を承認し、クラス証明書C_p3に含まれるクラス公開鍵K_{Pcp}3を受理する（ステップS408）。そして、次の処理（ステップS409）へ移行する。コントローラ214は、正当なクラス証明書でない場合には、クラス証明書C_p3を非承認とし、クラス証明書C_p3を受理せずにエラー通知を端末装置10へ出力し（ステップS435）、端末装置10においてエラー通知が受理されると（ステップS436）、再生許諾セッションが終了する。

【0229】

ステップS407における検証の結果、HD20において、再生回路150が正当なクラス証明書を持つ再生回路であることが確認され、ステップS408においてクラス公開鍵K_{Pcp}3が受理されると、HD20のセッション鍵発生部226は、セッション鍵K_{s1d}を生成する（ステップS409）。セッション鍵K_{s1d}は、受理されたクラス公開鍵K_{Pcp}3によって、暗号処理部222

において暗号化され、暗号化データE (K P c p 3, K s 1 d) が生成される (ステップS410)。

【0230】

そして、コントローラ214は、暗号処理部222からバスBS3を介して暗号化データE (K P c p 3, K s 1 d) を受けると、ATAインターフェース部212および端子210を介して端末装置10へ出力する (ステップS411)。

【0231】

端末装置10において、HDインターフェース部110およびバスBS2を介してコントローラ108が暗号データE (K P c p 3, K s 1 d) を受取ると (ステップS412)、コントローラ108は、受取した暗号化データE (K P c p 3, K s 1 d) をバスBS2を介して再生回路150へ出力する (ステップS413)。再生回路150の復号処理部1506は、バスBS2から暗号化データE (K P c p 3, K s 1 d) を受取ると (ステップS414)、K c p 保持部1504に保持される再生回路150に固有なクラス秘密鍵K c p 3によって復号処理することによりセッション鍵K s 1 dを復号し、セッション鍵K s 1 dが受取られる (ステップS415)。

【0232】

セッション鍵K s 1 dが受取られると、セッション鍵発生部1508は、セッション鍵K s 2 dを生成し (ステップS416)、生成したセッション鍵K s 2 dを暗号処理部1510に与える。暗号処理部1510は、復号処理部1506から受けるセッション鍵K s 1 dをセッション鍵K s 2 dにより暗号化し、暗号化データE (K s 1 d, K s 2 d) を生成する (ステップS417)。そして、暗号処理部1510は、暗号化データE (K s 1 d, K s 2 d) をバスBS2へ出力する (ステップS418)。

【0233】

コントローラ108は、バスBS2から暗号化データE (K s 1 d, K s 2 d) を受取し (ステップS419)、受取したデータをバスBS2およびHDインターフェース部110を介してHD20へ出力する (ステップS420)。

【0234】

HD20のコントローラ214は、端子210およびATAインターフェース部212を介して暗号化データE(Ks1d, Ks2d)を受理すると(ステップS421)、受理したデータをバスBS3へ出力する。復号処理部228は、セッション鍵発生部226から与えられたセッション鍵Ks1dを用いてバスBS3に出力された暗号化データE(Ks1d, Ks2d)を復号し、HD20においてセッション鍵Ks2dが受理される(ステップS422)。そして、コントローラ214は、セッション鍵Ks2dが受理されると、その旨の通知をATAインターフェース部212および端子210を介して端末装置10へ出力する。

【0235】

端末装置10のコントローラ108は、HDインターフェース部110およびバスBS2を介してHD20においてセッション鍵Ks2dが受理された旨の通知を受理すると、再生リクエストのあったコンテンツデータに対応する対象のライセンスLICが格納されているセキュアデータメモリ250AのLBAをバスBS2およびHDインターフェース部110を介してHD20へ出力する。

【0236】

HD20のコントローラ214は、端子210およびATAインターフェース部212を介して対象のライセンスLICが格納されているLBAを受理すると(ステップS424)、そのLBAに格納されるライセンスLICに対応する有効フラグメモリ250Cのフラグが「有効」であるか「無効」であるかを確認する(ステップS425)。

【0237】

コントローラ214は、有効フラグメモリ250Cのフラグが「有効」であると、受理したLBAに基づいて、対象のライセンスLICをセキュアデータメモリ250Aから取得する(ステップS426)。そして、コントローラ214は、取得したライセンスLICに含まれる制御情報ACの内容を確認する(ステップS427)。コントローラ214は、制御情報ACにおいて利用回数が指定されているときは、制御情報ACの利用回数を1増分し、次の処理(ステップS4

29)へ移行する。一方、コントローラ214は、制御情報ACにより再生制限がかけられていないときは、取得したライセンスLICに含まれるコンテンツ鍵KcをバスBS3へ出力する。

【0238】

暗号処理部224は、復号処理部228から受けるセッション鍵Ks2dによりバスBS3上に出力されたコンテンツ鍵Kcを暗号化して暗号化データE(Ks2d, Kc)を生成し(ステップS429)、生成したデータをバスBS3へ出力する。そして、コントローラ214は、バスBS3上に出力された暗号化データE(Ks2d, Kc)をATAインターフェース部212および端子210を介して端末装置10へ出力する(ステップS430)。

【0239】

端末装置10のコントローラ108は、HDインターフェース部110およびバスBS2を介して暗号化データE(Ks2d, Kc)を受理すると(ステップS431)、受理したデータをバスBS2へ出力する(ステップS432)。

【0240】

再生回路150の復号処理部1512は、バスBS2から暗号化データE(Ks2d, Kc)を受理すると(ステップS433)、セッション鍵発生部1508から与えられるセッション鍵Ks2dを用いて暗号化データE(Ks2d, Kc)を復号する。これにより、再生回路150においてコンテンツ鍵Kcが受理され(ステップS434)、一連の再生許諾セッションの処理が正常終了する。

【0241】

一方、ステップS425において、有効フラグメモリ250Cのフラグが「無効」であったとき、またはステップS427において、制御情報ACに含まれる内容が再生不可であったときは、コントローラ214は、端末装置10に対してエラー通知を出力し(ステップS435)、端末装置10においてエラー通知が受理されると(ステップS436)、再生許諾セッションが終了する。

【0242】

このようにして、データ記憶装置であるHD20から端末装置10に備えられる再生回路150への再生許諾に関しても、再生回路150が正規のクラス証明

書C p 3を保持していること、およびクラス証明書C p 3に含まれて送信されたクラス公開鍵K P c p 3が有効であることを確認した上でコンテンツ鍵K cが再生回路150へ送信され、不正なコンテンツデータの再生を禁止することができる。

【0243】

また、上述したように、ハードディスクにおいて相当数記憶されるライセンスをLBAにより管理することによって、再生許諾セッションにおいて、再生リクエストのあったコンテンツデータに対応するライセンスを、相当数のデータの中から検索することなくダイレクトに取得することができ、迅速な処理が実現できる。

【0244】

なお、フローチャートにおいて図示しないが、再生回路150は、コンテンツの再生許諾がなされ、コンテンツ鍵K cを受理すると、HD20から出力された暗号化コンテンツデータE (K c, D c)を復号処理部1514において復号し、再生部1516において復号処理部により復号されたデータD cが再生され、DA変換部1518によりデジタル／アナログ変換されてモニタやスピーカなどが接続される端子1520へ再生信号が出力される。

【0245】

なお、上述した全ての説明においては、コンテンツデータに対するライセンスについて説明したが、対象は、上述したライセンスに限られるものではなく、秘密にする必要がある機密データ一般に拡大されうる。上述した手段によって、データの機密性が保護され、かつ、データ記憶装置における機密データの特定に関する本発明の目的が達成できるからである。

【0246】

今回開示された実施の形態は、すべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図1】 データ配信システムを概念的に説明する概略図である。

【図2】 図1に示すデータ配信システムにおいて送受信されるデータ、情報等の特性を示す図である。

【図3】 図1に示すデータ配信システムにおいて使用される認証のためのデータ、情報等の特性を示す図である。

【図4】 図1に示すライセンス提供装置の構成を示す概略ブロック図である。

【図5】 図1に示す端末装置の構成を示す概略ブロック図である。

【図6】 図1に示す端末装置に装着されるハードディスクの構成を示す概略ブロック図である。

【図7】 図6に示すハードディスクにおけるセキュアデータ記憶部のメモリ構成を示す図である。

【図8】 図1に示すデータ配信システムにおける配信処理を説明するための第1のフローチャートである。

【図9】 図1に示すデータ配信システムにおける配信処理を説明するための第2のフローチャートである。

【図10】 図1に示すデータ配信システムにおける配信処理中の再書込処理を説明するための第1のフローチャートである。

【図11】 図1に示すデータ配信システムにおける配信処理中の再書込処理を説明するための第2のフローチャートである。

【図12】 図1に示すデータ配信システムにおける配信処理中の再書込処理を説明するための第3のフローチャートである。

【図13】 複製・移動処理が行なわれるシステム構成を概念的に説明する概略図である。

【図14】 図13に示すシステムにおける複製または移動処理を説明するための第1のフローチャートである。

【図15】 図13に示すシステムにおける複製または移動処理を説明するための第2のフローチャートである。

【図16】 図13に示すシステムにおける複製または移動処理中の再書込

処理を説明するための第1のフローチャートである。

【図17】 図13に示すシステムにおける複製または移動処理中の再書込処理を説明するための第2のフローチャートである。

【図18】 図13に示すシステムにおける複製または移動処理中の再書込処理を説明するための第3のフローチャートである。

【図19】 図5に示す端末装置に対する再生許諾処理を説明するためのフローチャートである。

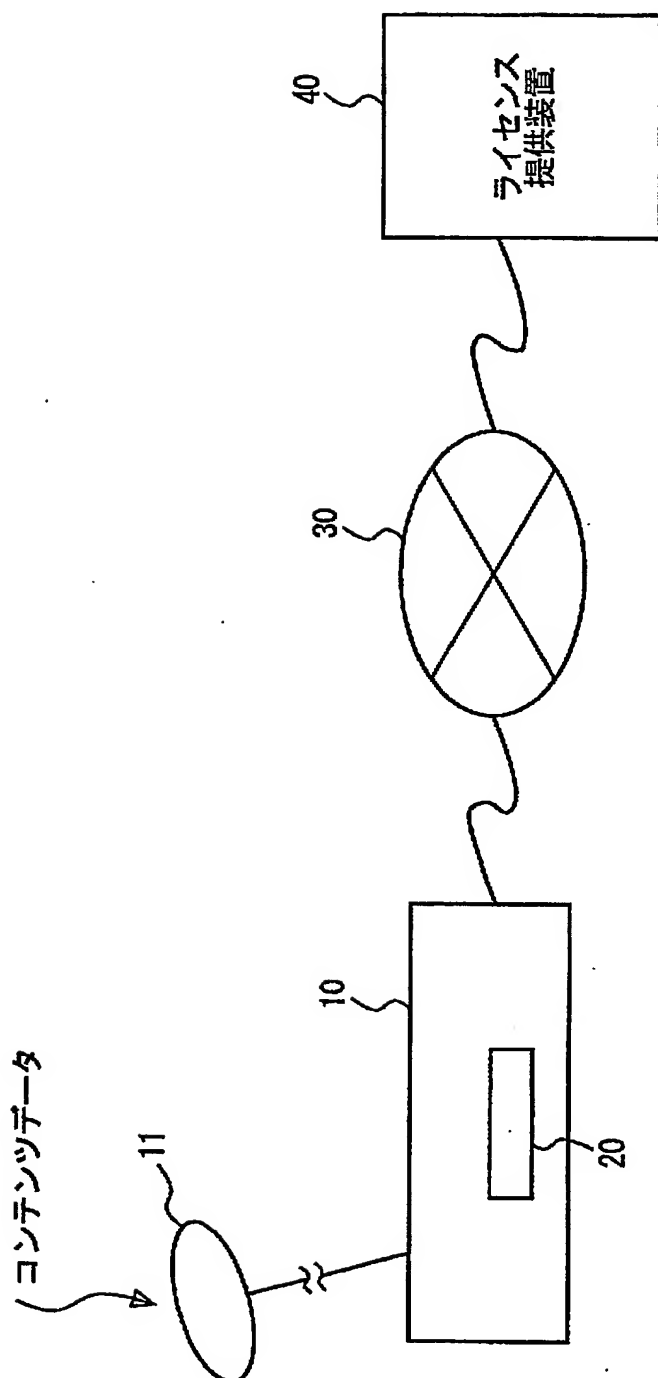
【符号の説明】

10 端末装置、11 アンテナ、20, 21 ハードディスク、30 ネットワーク、40 ライセンス提供装置、102 アンテナ、104 受信部、106 モデム、108 コントローラ、110 HDインターフェース部、150 再生回路、202, 1502 認証データ保持部、204 Kcm保持部、206 Kom保持部、208 KPom保持部、210, 1520 端子、212 ATAインターフェース部、214 コントローラ、216, 228, 230, 422, 1506, 1512, 1514 復号処理部、218, 416 KPa保持部、220, 418 認証部、222, 224, 232, 420, 424, 426, 1510 暗号処理部、226, 414, 1508 セッション鍵発生部、250 セキュアデータ記憶部、250A セキュアデータメモリ、250B ログメモリ、250C 有効フラグメモリ、260, 262 切替スイッチ、270 ノーマルデータ記憶部、402 コンテンツDB、404 ログDB、410 データ処理部、412 配信制御部、450 通信装置、1504 Kcp保持部、1516 再生部、1518 DA変換部、2501 ライセンスID領域、2502 Ks2x領域、2503 ST1領域、2504 ST2領域、2505 KPcmx領域、2506 LBA領域、2701 磁気記録媒体、2702 モータ、2703 サーボ制御部、2704 シーク制御部、2705 記録再生処理部、BS1～BS3 バス。

【書類名】

図面

【図 1】



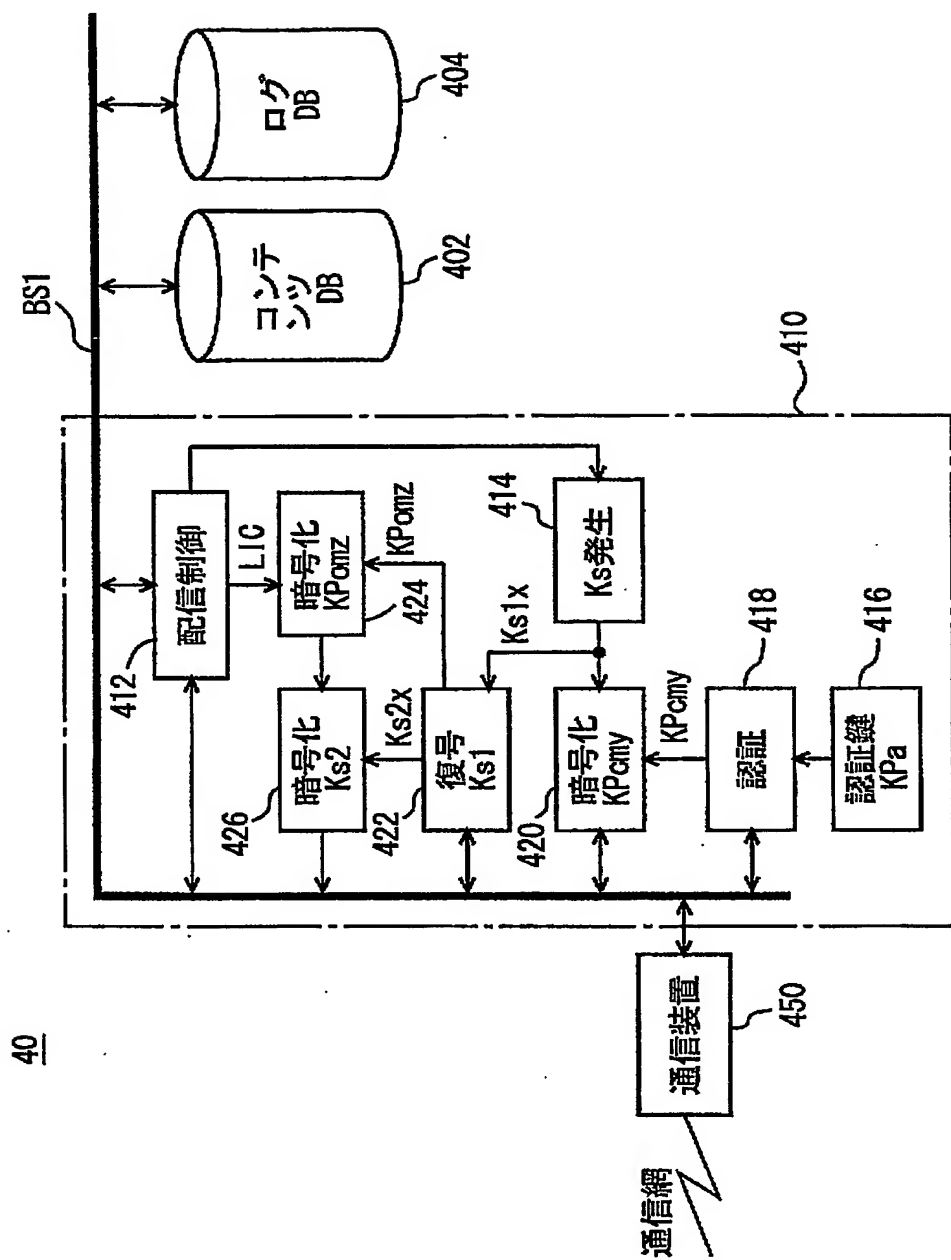
【図 2】

記号	名称	属性	特性
Dc	データ	データ固有	例：映像データ、音楽データ、朗読データ、教材データ、 画像データ、ゲームプログラム Kcにて暗号化した暗号化コンテンツデータ E(Kc, Dc)として記録管理される
Di	データ情報	データ固有	Dcに付随する平文データ。DIDを含む
DID	データID	データ固有	DcおよびKcを特定するための管理コード
Kc	コンテンツ鍵	データ固有	暗号データを暗号／復号する共通鍵
AC	制御情報	ライセンス固有	再生やライセンスの取扱いに関する制限事項
LID	ライセンスID	ライセンス固有	ライセンスを特定するための管理コード
LIC	ライセンス	ライセンス固有	Kc//AC//DID//LIDの総称

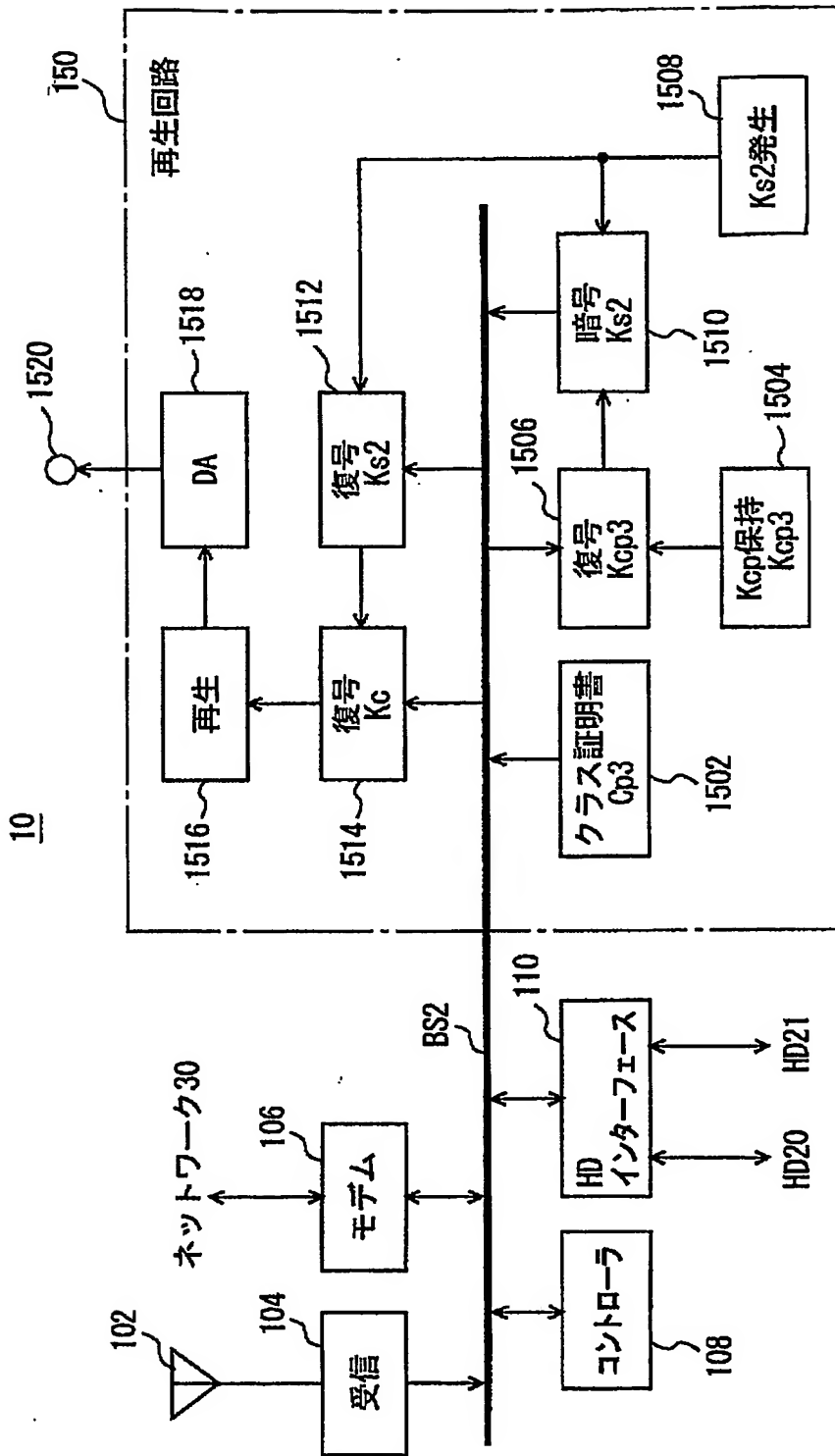
【図3】

記号	名称	特性
ライセンサ提供装置	認証鍵	認証局にて証明書を検証する公開復号鍵 ライセンサ提供側にて運用される
	Ks1x	セッション鍵 ライセンサの配信ごとに生成される一時鍵 共通鍵
	Ka	マスタ鍵 クラス証明書作成のために使用する秘密暗号鍵 認証局にて運用される
	KPa	認証鍵 認証局にて証明書を検証する公開復号鍵 ライセンサ提供側にて運用される
データ記録装置 (ハードディスク)	KPcmy	機器のクラス(種類などの一定の単位ごと)に付与される暗号鍵 Iylはクラスを識別するための識別子
	Kcmv	クラス公開鍵KPcmyにて暗号化されたデータを復号する非対称な復号鍵
	Icmv	クラスごとの機器およびクラス公開鍵に関する情報データ
	Qmy	$Qmy = KPcmy // Icmv // E(Ka, H(KPcmy // Icmv))$ 認証鍵KPaによってその正当性が確認できる
	KPcmz	データ記録装置ごとに固有な値を持つ個別公開暗号鍵 Izlはデータ記録装置を識別するための識別子
	Kcmz	個別公開鍵KPcmzにて暗号化されたデータを復号する非対称な復号鍵
	Ks1x	セッション鍵 ライセンサの授受ごとにライセンサ提供側で生成される一時鍵 共通鍵
	Ks2x	セッション鍵 ライセンサの授受ごとにライセンサ受理側で生成される一時鍵 共通鍵
再生回路	KPcpy	機器のクラス(種類などの一定の単位ごと)に付与される暗号鍵 Iylはクラスを識別するための識別子
	Kopy	クラス公開鍵KPcpyにて暗号化されたデータを復号する非対称な復号鍵
	Icpy	クラスごとの機器およびクラス公開鍵に関する情報データ
	Qpy	$Qpy = KPcpy // Icpy // E(Ka, H(KPcpy // Icpy))$ 認証鍵KPaによってその正当性が確認できる
	Ks2x	セッション鍵 ライセンサの授受ごとにライセンサ受理側で生成される一時鍵 共通鍵

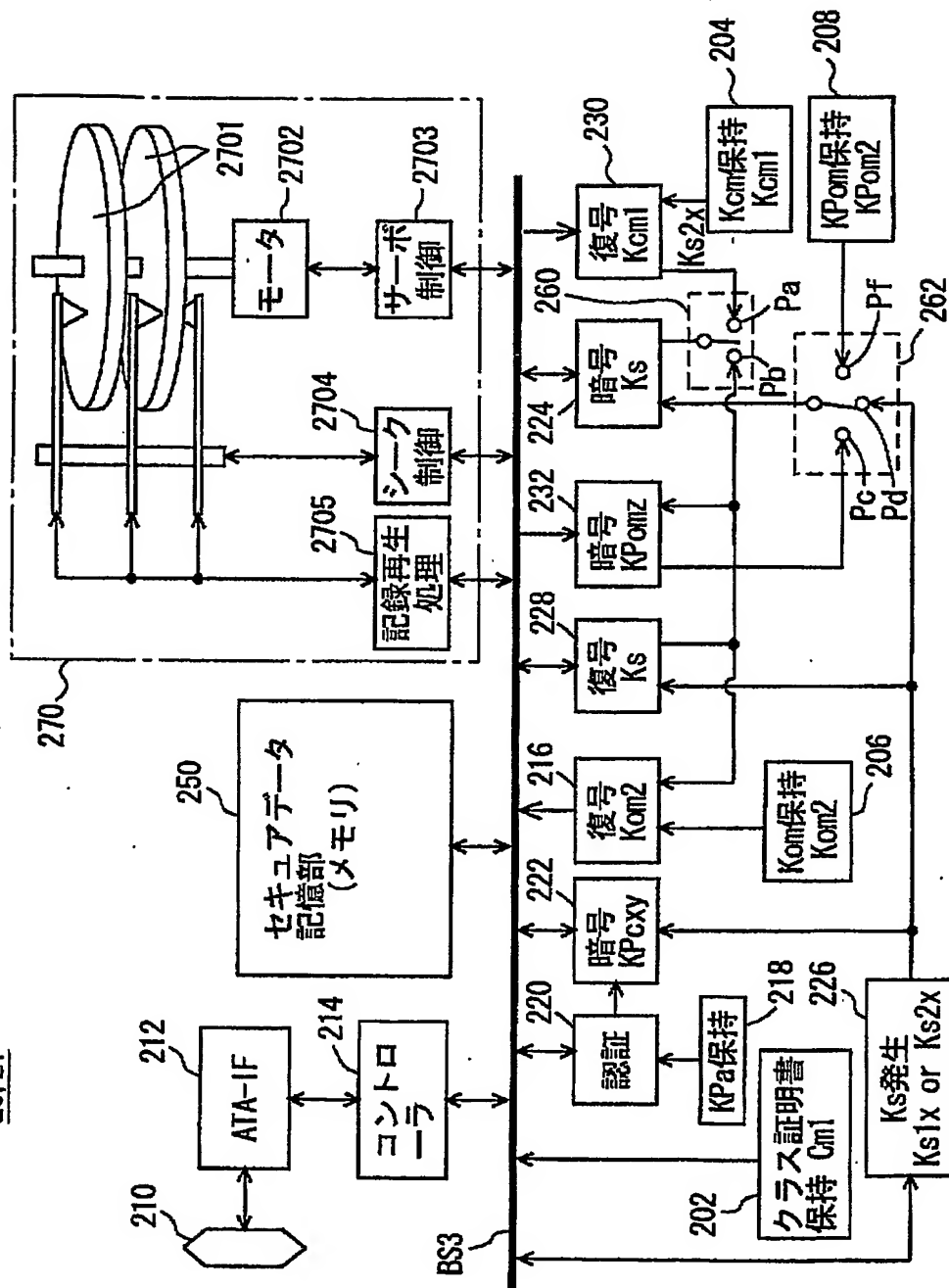
【图 4】



【図 5】

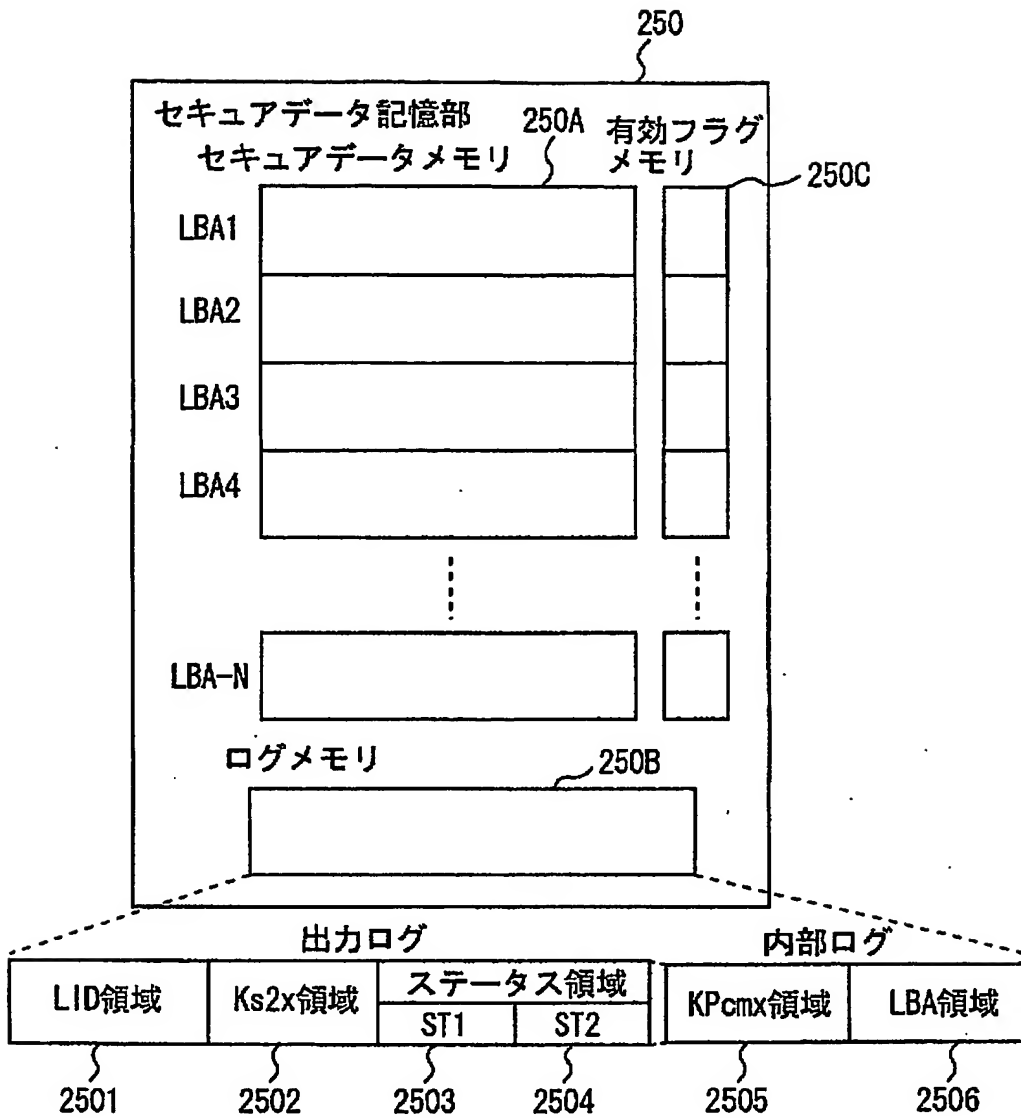


【图 6】

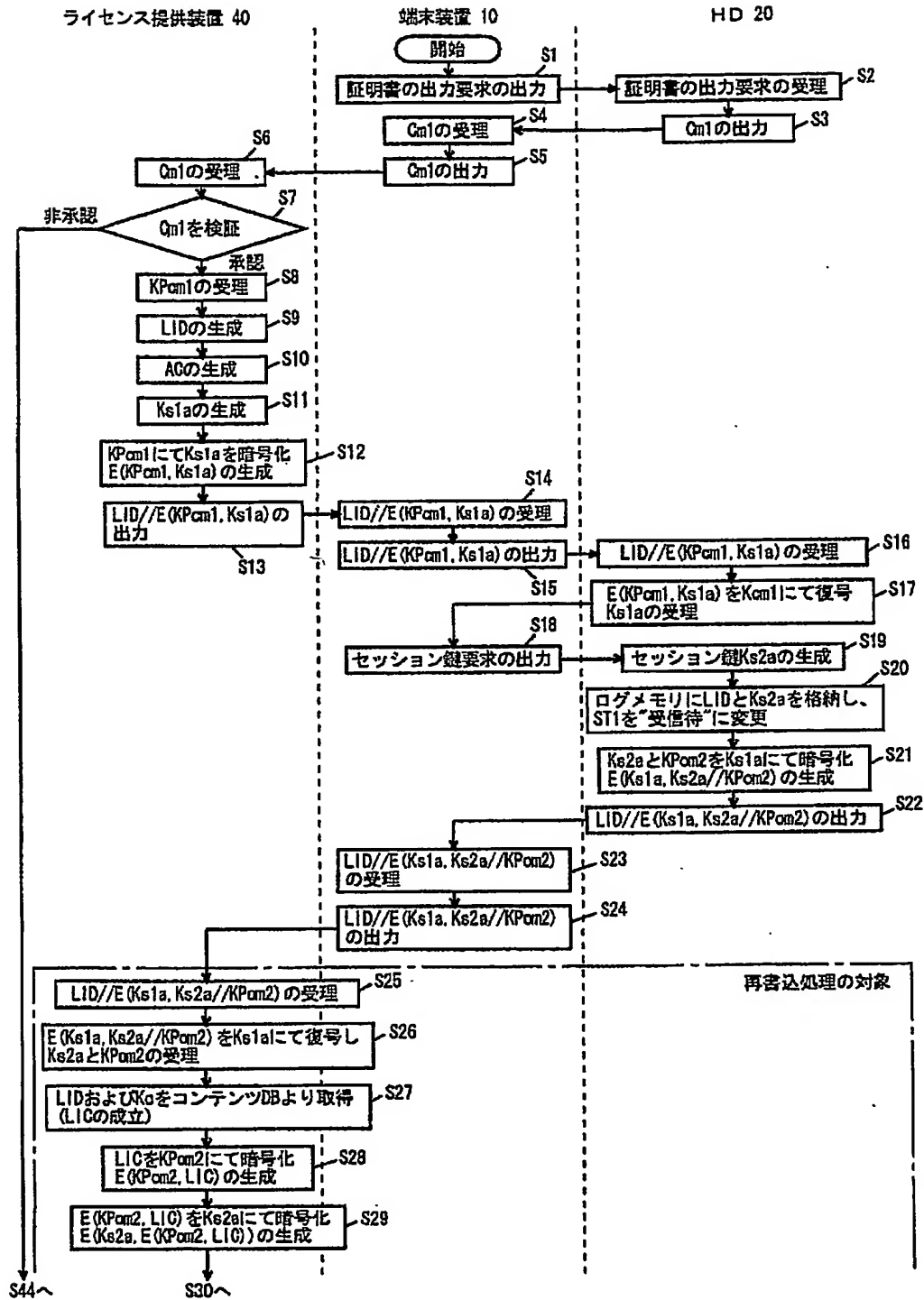


20, 21

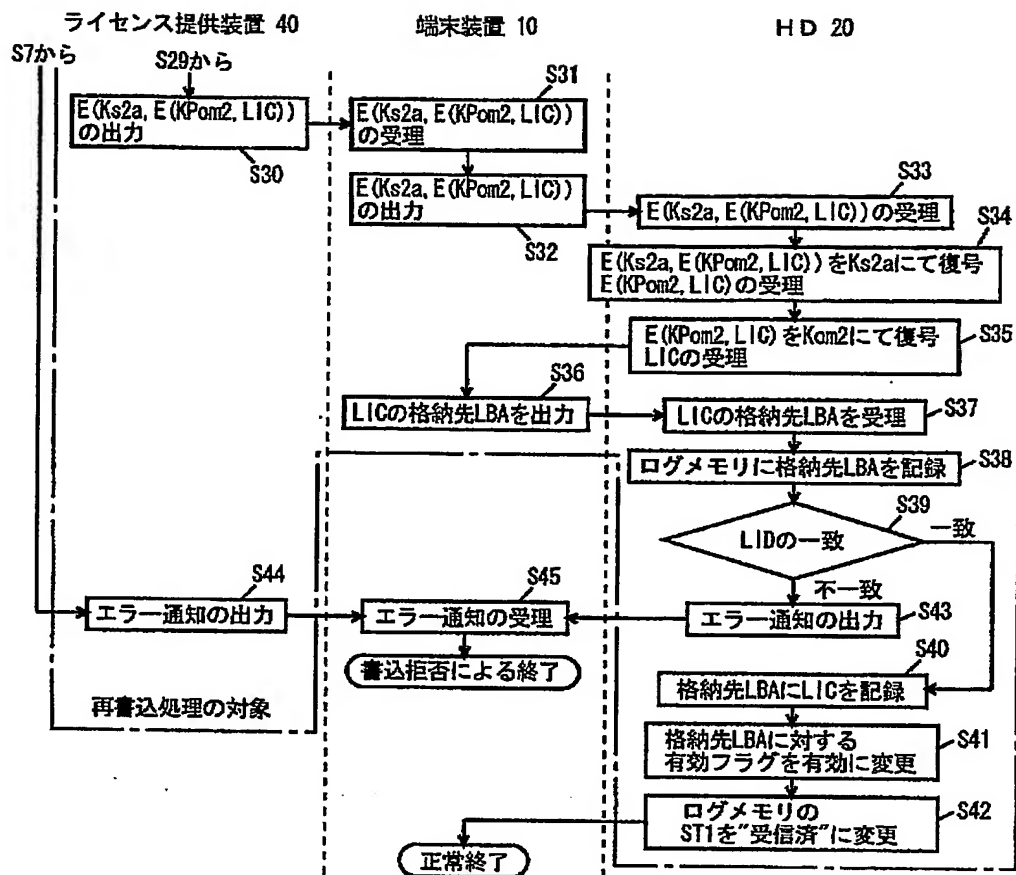
【図 7】



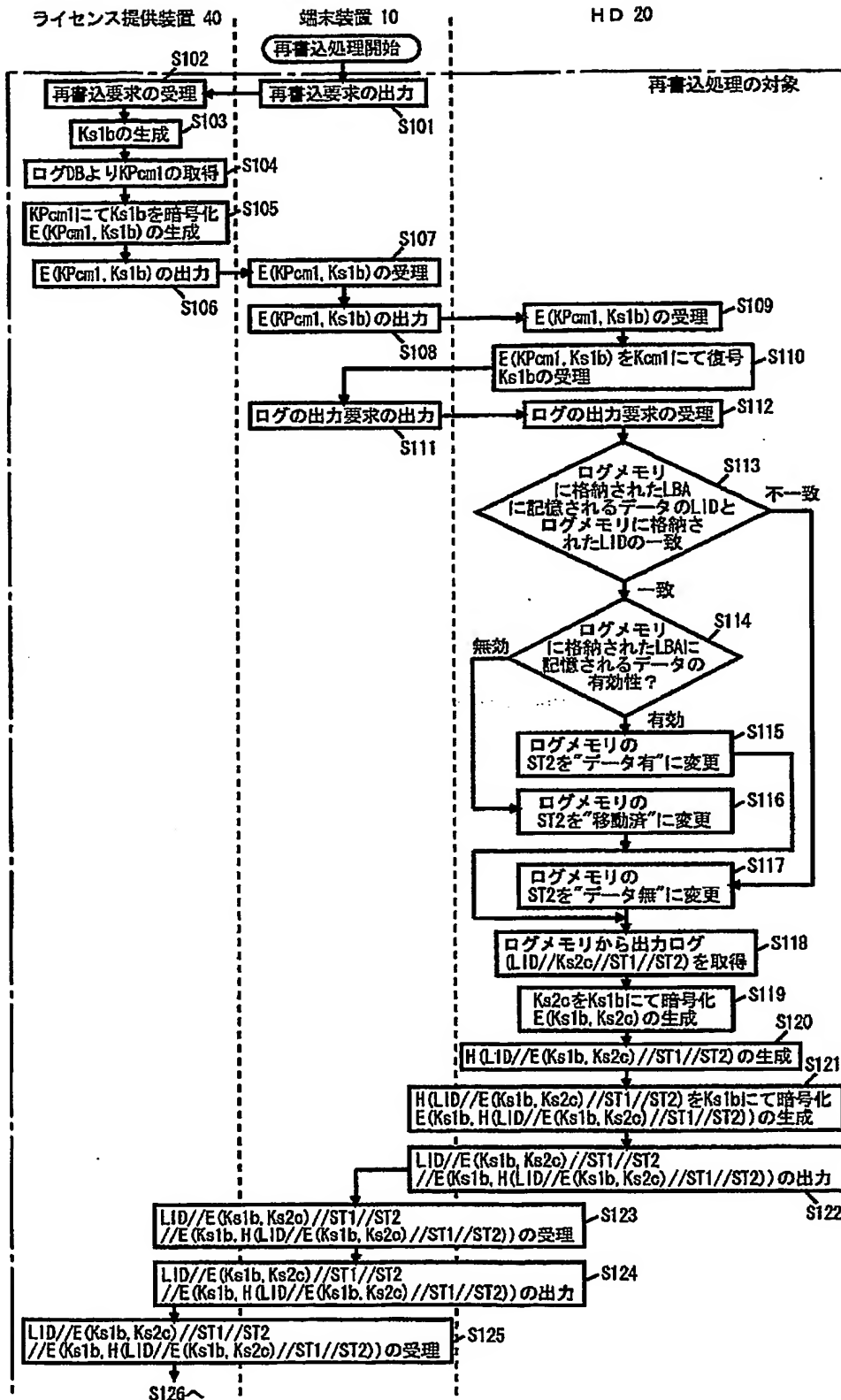
【図 8】



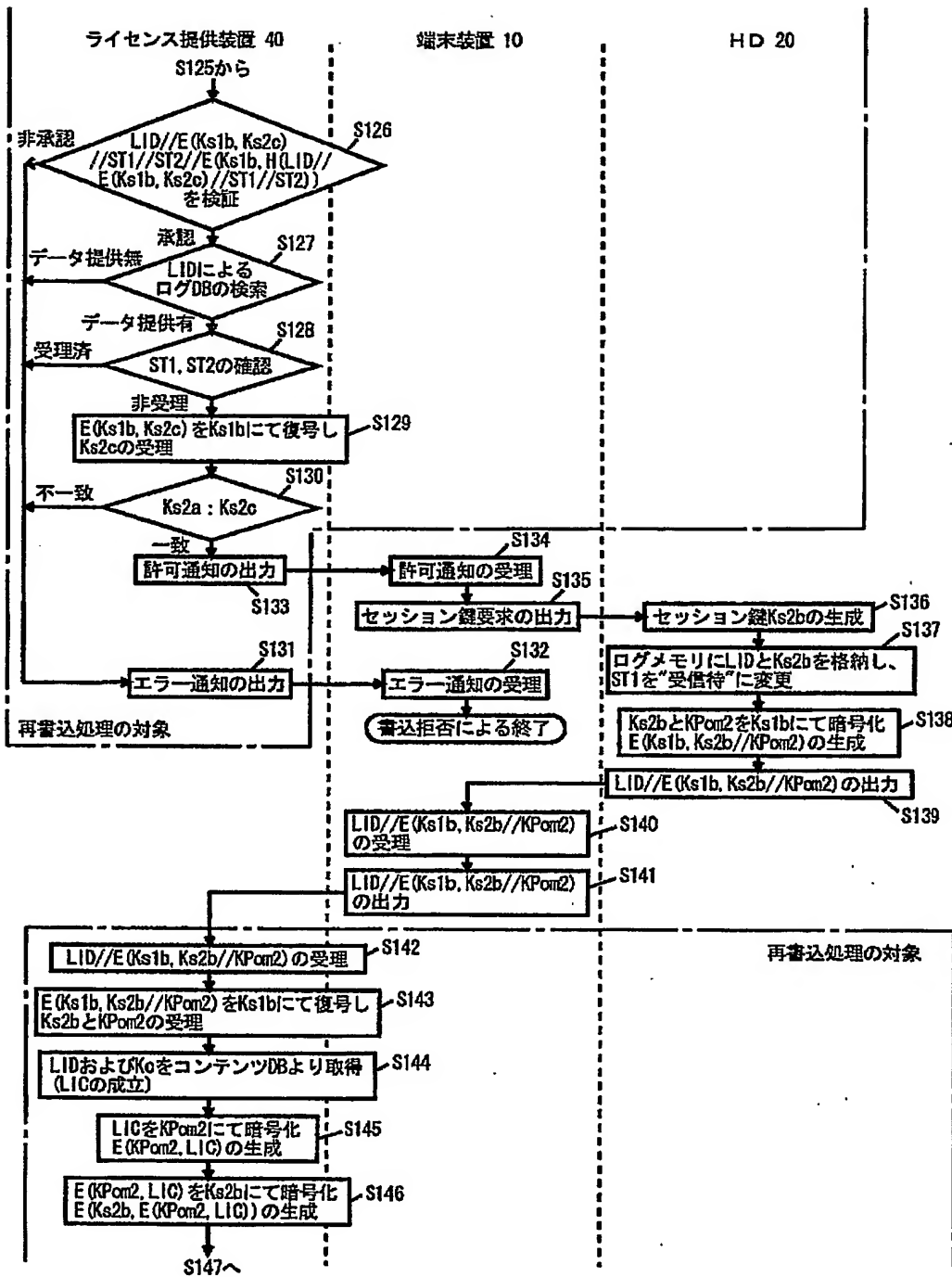
【図 9】



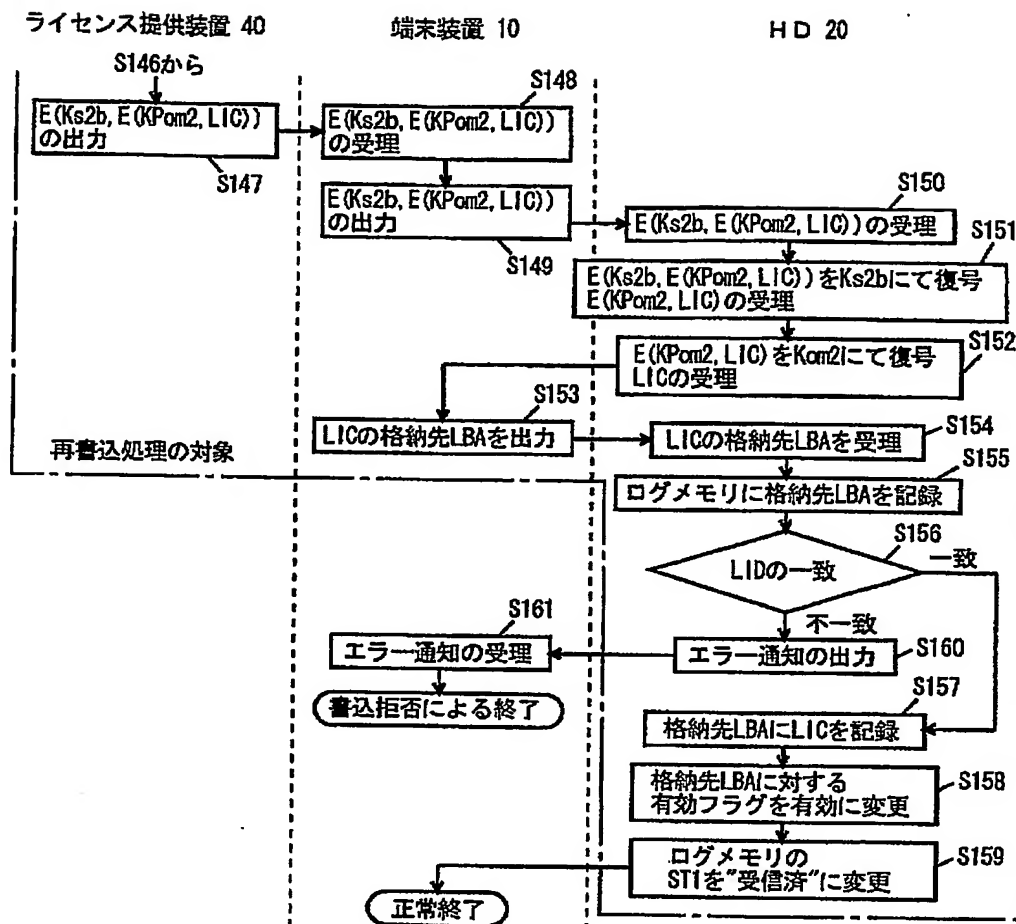
【図 10】



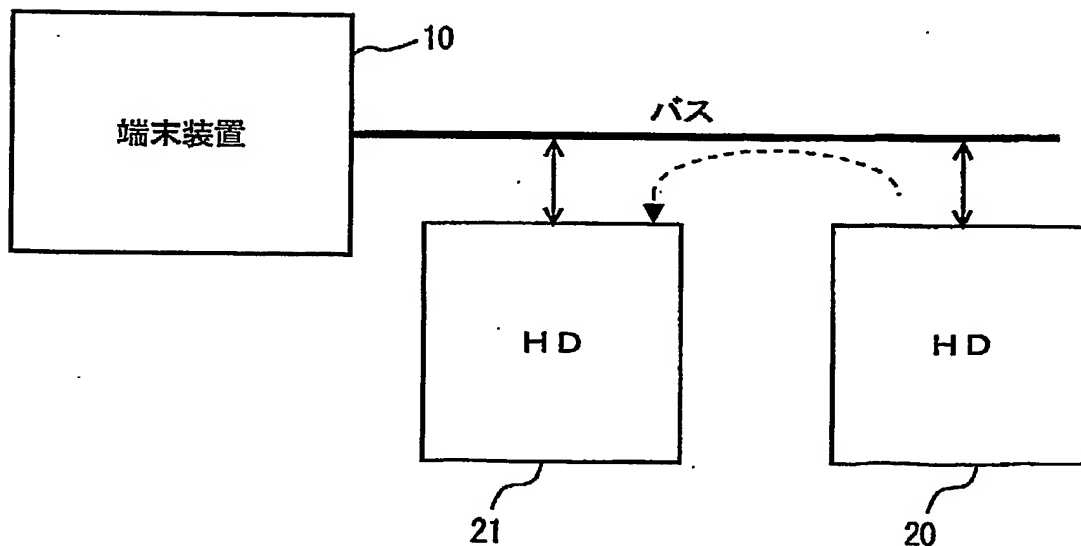
【図 11】



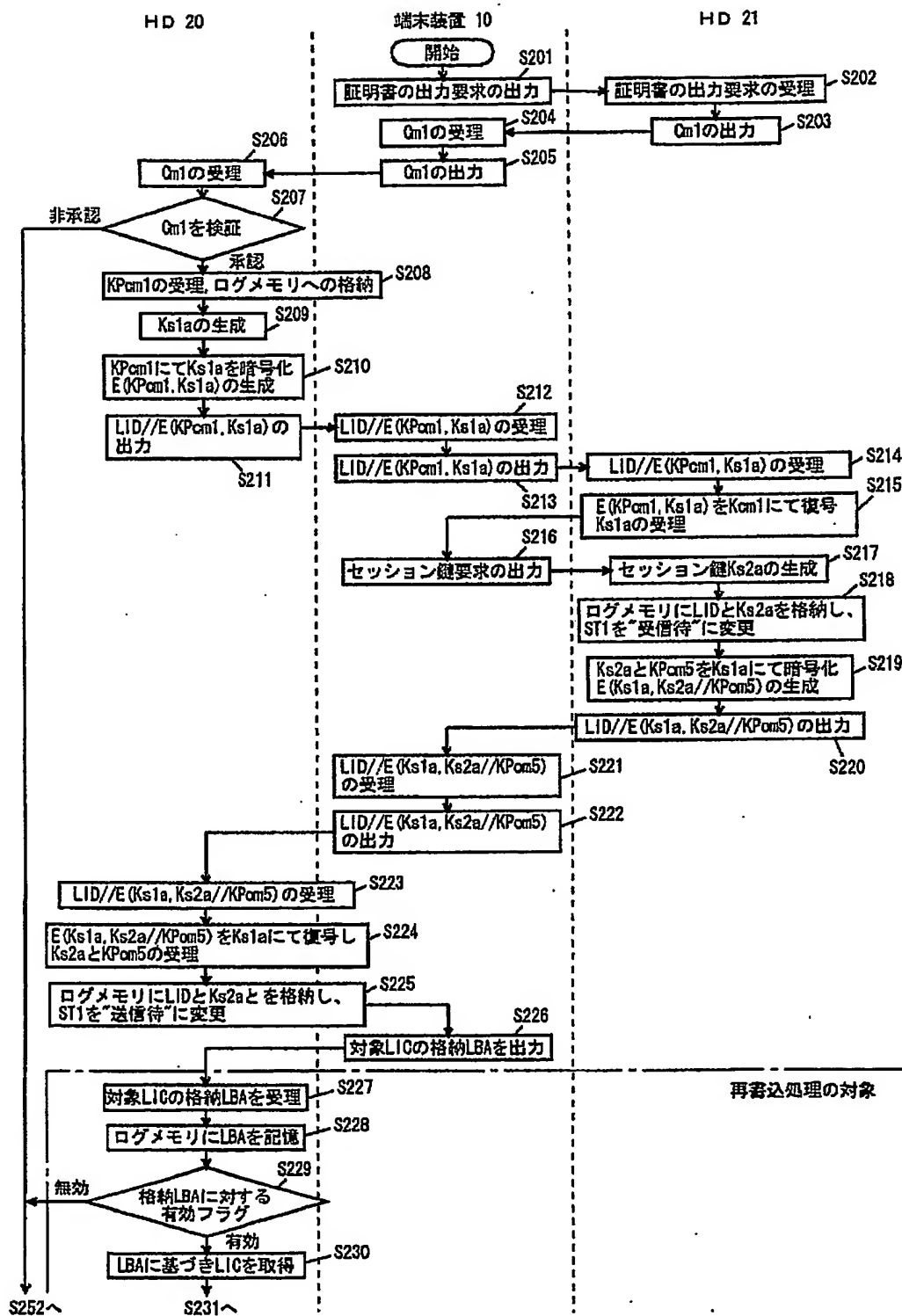
【図 1 2】



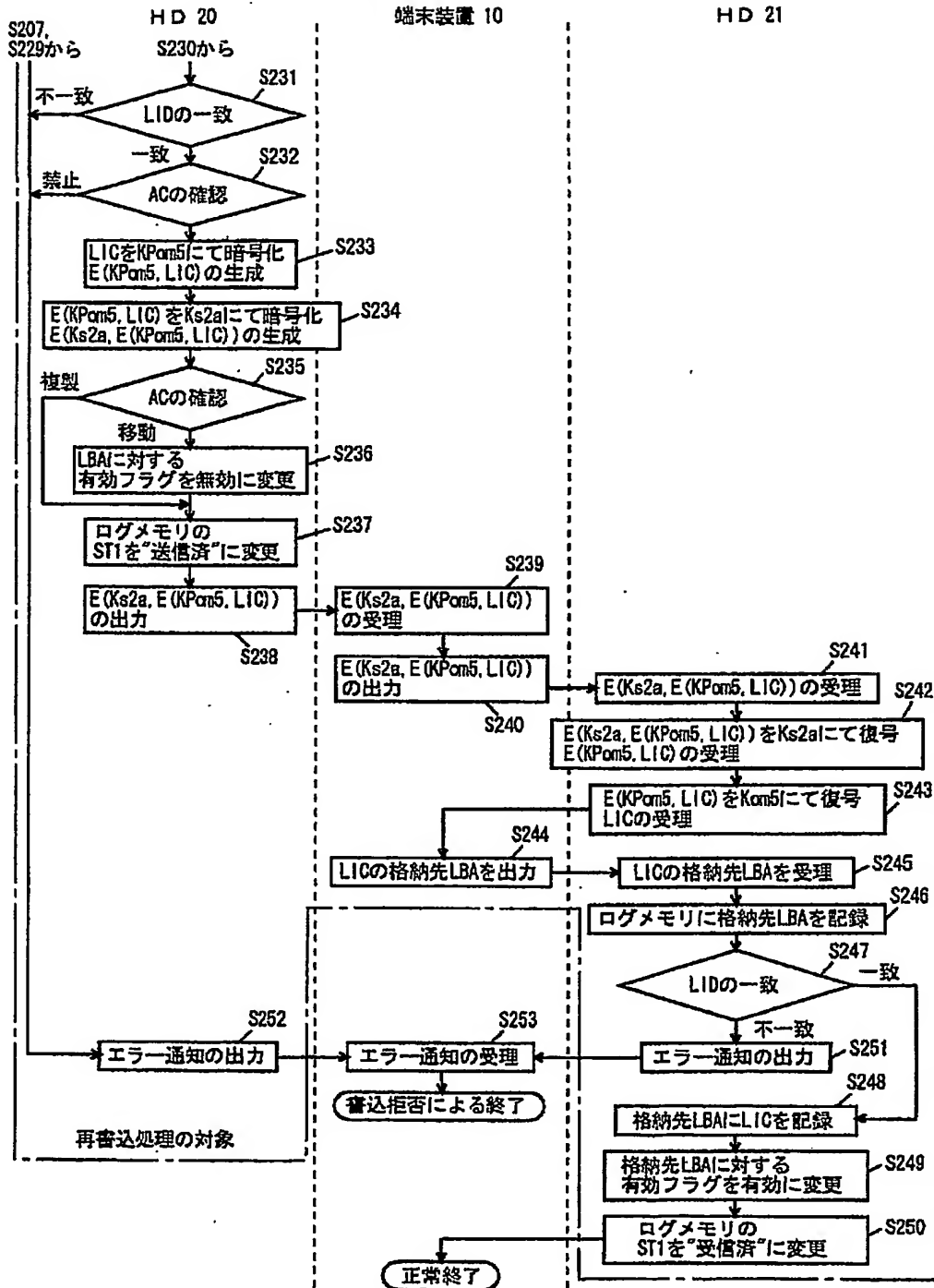
【図 1 3】



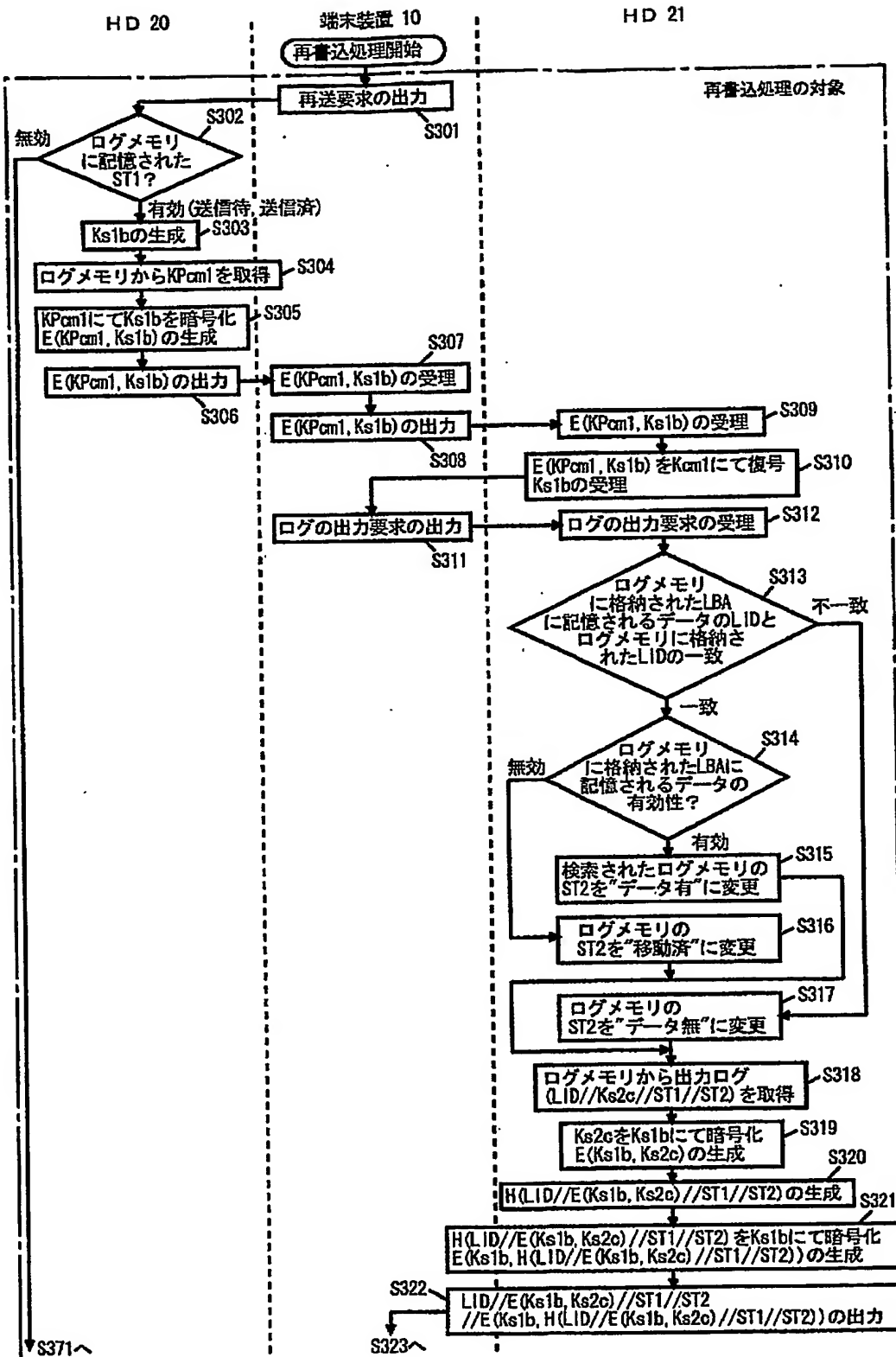
【図 14】



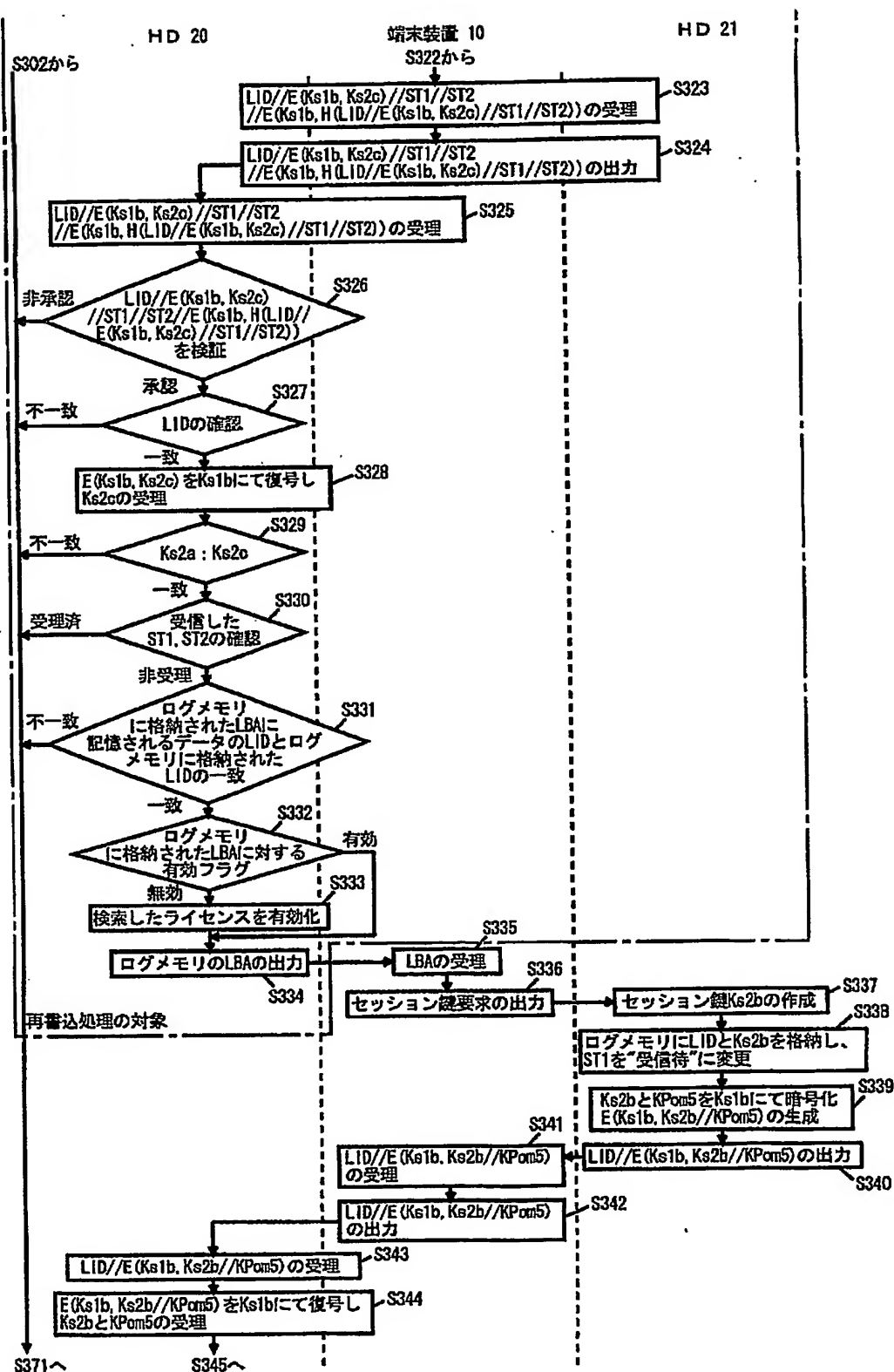
【図 15】



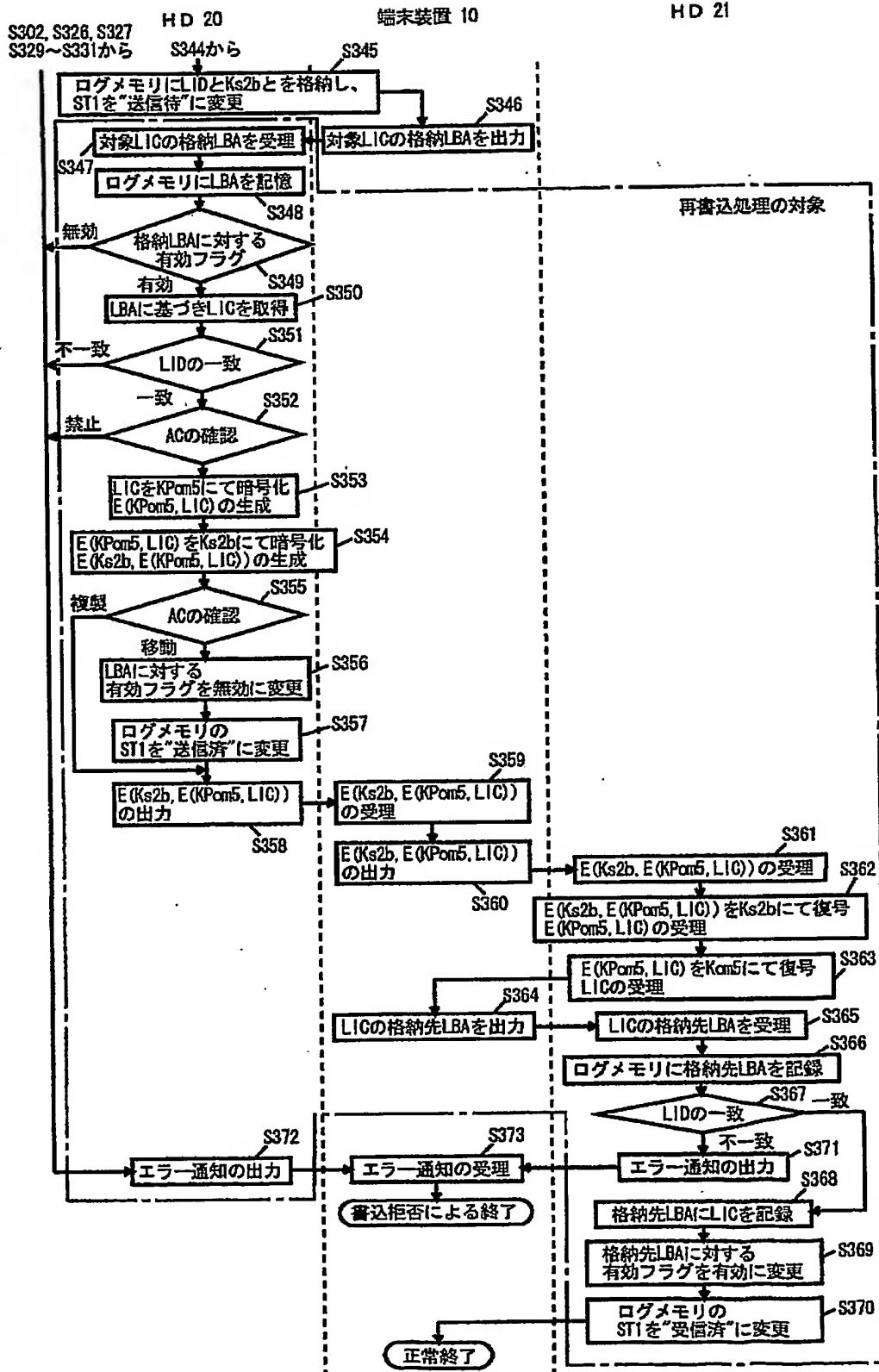
【図 16】



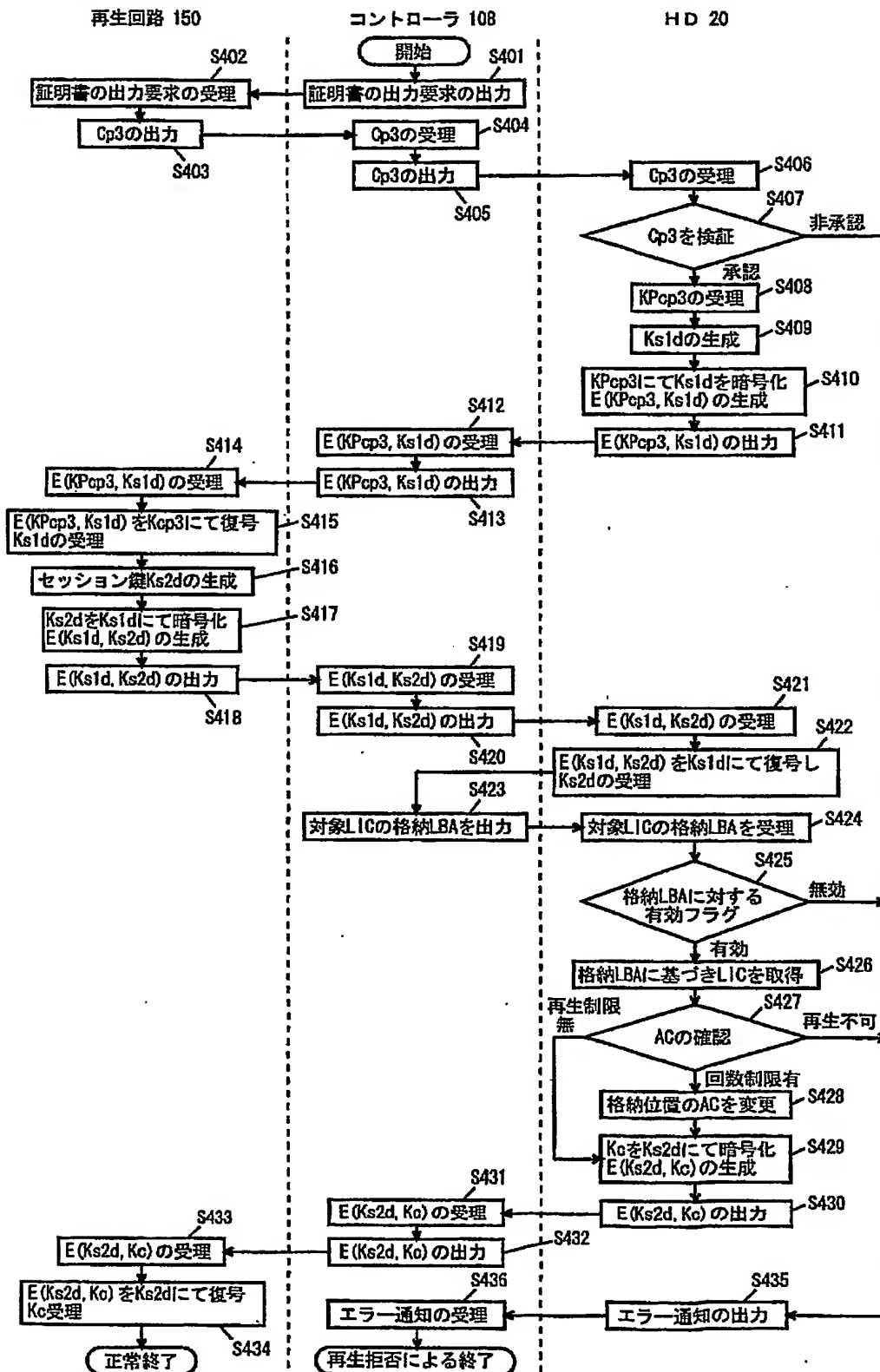
【図 17】



【図 18】



【図 19】



【書類名】 要約書

【要約】

【課題】 相当数記録されたライセンスの中から送受信処理中のライセンスを迅速に特定でき、特にライセンスの送受信処理中に異常が発生したときに、ライセンスの保護と再処理の高速化とを両立するデータ記録装置を提供する。

【解決手段】 データ記録装置としてのHD（ハードディスク）20，21におけるコントローラ214は、暗号化コンテンツデータを復号するためのコンテンツ鍵などを含むライセンスをセキュアデータ記憶部250に記憶する。ライセンスは、セキュアデータ記憶部250内においてLBA（アドレス情報）によって管理され、また、送受信処理中のライセンスが格納されるLBAがログとしてセキュアデータ記憶部250内のログメモリに格納される。そして、送受信処理中に異常が発生したときは、ログメモリに格納されたLBAに基づいて送受信処理中であったライセンスが特定される。

【選択図】 図6

出 願 人 履 歴 情 報

識別番号 [000001889]

1. 変更年月日	1993年10月20日
[変更理由]	住所変更
住 所	大阪府守口市京阪本通2丁目5番5号
氏 名	三洋電機株式会社

出 願 人 履 歴 情 報

識別番号 [000005049]

1. 変更年月日	1990年 8月29日
[変更理由]	新規登録
住 所	大阪府大阪市阿倍野区長池町22番22号
氏 名	シャープ株式会社

出 願 人 履 歴 情 報

識別番号 [000004329]

1. 変更年月日	1990年 8月 8日
[変更理由]	新規登録
住 所	神奈川県横浜市神奈川区守屋町3丁目12番地
氏 名	日本ビクター株式会社

出 願 人 履 歴 情 報

識別番号 [000005016]

1. 変更年月日	1990年 8月31日
[変更理由]	新規登録
住 所	東京都目黒区目黒1丁目4番1号
氏 名	パイオニア株式会社

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日 1990年 8月31日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地
氏 名 株式会社日立製作所

出 願 人 履 歴 情 報

識別番号 [300017636]

1. 変更年月日 2000年 2月28日
 [変更理由] 新規登録
 住 所 東京都新宿区新宿4-2-18 新宿光風ビル6F
 氏 名 フェニックステクノロジーズ株式会社
2. 変更年月日 2002年 4月 4日
 [変更理由] 住所変更
 住 所 東京都千代田区丸の内1-3-1 東京銀行協会ビル14F
 氏 名 フェニックステクノロジーズ株式会社
3. 変更年月日 2002年 8月16日
 [変更理由] 住所変更
 住 所 東京都新宿区新宿4-2-18 新宿光風ビル6F
 氏 名 フェニックステクノロジーズ株式会社
4. 変更年月日 2003年 1月 8日
 [変更理由] 住所変更
 住 所 東京都千代田区丸の内1-3-1 東京銀行協会ビル14F
 氏 名 フェニックステクノロジーズ株式会社

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号

氏 名 富士通株式会社

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.